A QUESTION OF TRUST

REPORT OF THE INVESTIGATORY POWERS REVIEW

by

DAVID ANDERSON Q.C.
Independent Reviewer of Terrorism Legislation

JUNE 2015

Presented to the Prime Minister
pursuant to section 7 of the
Data Retention and Investigatory Powers Act 2014

A QUESTION OF TRUST

REPORT OF THE INVESTIGATORY POWERS REVIEW

by

DAVID ANDERSON Q.C.
Independent Reviewer of Terrorism Legislation

JUNE 2015

Presented to the Prime Minister
pursuant to section 7 of the
Data Retention and Investigatory Powers Act 2014

© Crown copyright 2015

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to the Independent Reviewer of Terrorism Legislation at independent.reviewer@brickcourt.co.uk or by post to David Anderson Q.C. at Brick Court Chambers, 7-8 Essex Street, London WC2R 3LD.

This document is also available from the Independent Reviewer's website at https://terrorismlegislationreviewer.independent.gov.uk

Print ISBN 9781474119450

Web ISBN 9781474119467

ID 20051503 06/15

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

OUTLINE CONTENTS

	Page
EXECUTIVE SUMMARY	1
DETAILED CONTENTS	10
PART I: BACKGROUND	
1. INTRODUCTION	15
2. PRIVACY	25
3. THREATS	39
4. TECHNOLOGY	49
PART II: CURRENT POSITION	
5. LEGAL CONSTRAINTS	71
6. POWERS AND SAFEGUARDS	95
7. PRACTICE	124
8. COMPARISONS	141
PART III: PERSPECTIVES AND VISIONS	
9. LAW ENFORCEMENT	166
10. INTELLIGENCE	190
11. SERVICE PROVIDERS	203
12. CIVIL SOCIETY	213
PART IV: CHARTING THE FUTURE	
13. PRINCIPLES	245
14. EXPLANATIONS	257
15. RECOMMENDATIONS	285

LIST OF ANNEXES

		Page
Annex 1:	List of Acronyms	308
Annex 2:	Defined terms	313
Annex 3:	Submissions	315
Annex 4:	Meetings	317
Annex 5:	Impact of encryption and anonymisation	321
Annex 6:	Bodies with non-RIPA powers	323
Annex 7:	The Snowden allegations	330
Annex 8:	Interception case studies	334
Annex 9:	Bulk data case studies	337
Annex 10:	UK Retained communications data case studies	339
Annex 11:	Crime types for which communications data is used	342
Annex 12:	Urgency of requirements for communications data	343
Annex 13:	Local authority use of communications data	344
Annex 14:	Local authority RIPA requests via NAFN	348
Annex 15:	The law of the Five Eyes	349
Annex 16:	Potential use of traffic data by local authorities	370
Annex 17:	ISIC Model A	372
Annex 18:	ISIC Model B	373

EXECUTIVE SUMMARY

INTRODUCTION

1. As Independent Reviewer of Terrorism Legislation, I am required by the Data Retention and Investigatory Powers Act 2014 to examine

   a. the threats to the United Kingdom,

   b. the capabilities required to combat those threats,

   c. the safeguards to protect privacy,

   d. the challenges of changing technologies, and

   e. issues relating to transparency and oversight,

   before reporting to the Prime Minister on the effectiveness of existing legislation relating to investigatory powers, and to examine the case for a new or amending law.

2. The scope of this task extends well beyond the field of counter-terrorism. Public authorities intercept communications, and collect information about communications, for a host of other purposes including counter-espionage, counter-proliferation, missing persons investigations and the detection and prosecution of both internet-enabled crime (fraud, cyber-attacks, child sexual exploitation) and crime in general.

3. The purpose of this Report is:

   a. to ***inform the public and political debate*** on these matters, which at its worst can be polarised, intemperate and characterised by technical misunderstandings; and

   b. to set out my own ***proposals for reform***, in the form of five governing principles and 124 specific recommendations.

4. In conducting my Review I have enjoyed unrestricted access, at the highest level of security clearance, to the responsible Government Departments (chiefly the Home Office and FCO) and to the relevant public authorities including police, National Crime Agency and the three security and intelligence agencies: MI5, MI6 and GCHQ. I have balanced those contacts by engagement with service providers, independent technical experts, NGOs, academics, lawyers, judges and regulators, and by fact-finding visits to Berlin, California, Washington DC, Ottawa and Brussels.

INFORMING THE DEBATE

5. The legal, factual and technological position as I understand it from my reading, my visits and the large number of interviews I have conducted is set out in the first 12 Chapters of this Report.

6. **Part I of the report (BACKGROUND)** establishes the context for the Review, explores the central concept of privacy and considers both current and future threats to the UK and the challenges of changing technology.

   a. **Chapter 1 (INTRODUCTION)** sets out the scope, aims and methodology of the Review.

   b. **Chapter 2 (PRIVACY)** looks at the importance of privacy for individual, social and political life. It charts attitudes to privacy and surveillance as they have evolved over time and as they have recently been captured in court judgments and in survey evidence from the UK and elsewhere.

   c. **Chapter 3 (THREAT)** looks at the importance of security for individual, social and political life. It assesses the threat to the UK in terms of both national security and crime, and puts it into a long-term perspective.

   d. **Chapter 4 (TECHNOLOGY)** explains the basic technology that underlies the debate, from changing methods of communication and new capabilities to encryption, anti-surveillance tools and the dark net.

7. **Part II of the Report (CURRENT POSITION)** explains the international legal backdrop, the current powers and the way in which they are used.

   a. **Chapter 5 (LEGAL CONSTRAINTS)** sets out the legal framework which governs action in this field. In the absence of a written constitution, the chief limitations on freedom to legislate are those imposed by the ECHR and (within its field of application) EU law.

   b. **Chapter 6 (POWERS AND SAFEGUARDS)** summarises the existing UK laws under which public authorities may collect and analyse people's communications, or records of their communications. It introduces the key concepts and summarises the various powers both under RIPA and outside it, together with the principal oversight mechanisms.

   c. **Chapter 7 (PRACTICE)** explains how those powers are applied in practice by intelligence, police, law enforcement and others, touching also on data-sharing, bulk personal datasets and the recently-avowed capability for computer network exploitation.

   d. **Chapter 8 (COMPARISONS)** provides three sets of benchmarks which may assist in working out how UK law on Investigatory Powers should look. These are:

      - ***other forms of surveillance*** (directed and intrusive surveillance, property interference, covert human intelligence sources etc.),

      - the laws of ***other countries***, particularly in Europe and the English-speaking world, and

- the use made of individuals' communications by service providers, retailers and other ***private companies***.

8. **Part III of the Report (PERSPECTIVES AND VISIONS)** draws on the submissions and evidence received by the Review in order to summarise the wishes of interested parties.

   a. **Chapter 9 (LAW ENFORCEMENT)** summarises the requirements of the NCA, police, local authorities and other law enforcement bodies. It addresses the utility of interception and communications data for their work, and their views on capabilities and safeguards.

   b. **Chapter 10 (INTELLIGENCE)** summarises the submissions made to the Review by the security and intelligence agencies: MI5, MI6 and GCHQ. It explains their views on technological change and encryption, what they say they need to maintain existing access and their priorities in relation to capabilities and authorisation of warrants.

   c. **Chapter 11 (SERVICE PROVIDERS)** summarises the submissions made to the Review by communications service providers, both in the US (regarding cooperation with the UK Government and extraterritorial effect) and in the UK (where there was a strong emphasis on the strengthening of controls and oversight).

   d. **Chapter 12 (CIVIL SOCIETY)** summarises the case made to the Review by civil society groups and individuals, some of whom challenged the need for current capabilities, and most of whom emphasised what they saw as the need for transparency, coherence and clarity and improved scrutiny and safeguards.

PROPOSALS FOR REFORM

9. **Part IV of the Report (CHARTING THE FUTURE)** contains my proposals for change.

   a. **Chapter 13 (PRINCIPLES)** characterises the key issue as one of trust, and sets out the five principles on which my recommendations are founded:

      - Minimise no-go areas
      - Limited powers
      - Rights compliance
      - Clarity
      - Unified approach.

      Under the fifth principle, I explain my reasons for rejecting the ISC's recommendation that the law in this area should, for the first time, enshrine a clear separation between intelligence and law enforcement functions.

b. **Chapter 14 (EXPLANATIONS)** is a commentary on the principal recommendations set out in Chapter 15. It explains my thinking on key issues such as:

- Defining content and communications data
- Compulsory data retention
- The proposals in the 2012 Communications Data Bill
- Bulk collection and bulk warrants
- Specific interception warrants
- Judicial authorisation
- Collection of communications data
- Extraterritorial effect
- Use of intercepted material and data
- The Independent Surveillance and Intelligence Commission (ISIC)
- The IPT
- Transparency.

c. **Chapter 15 (RECOMMENDATIONS)** sets out my 124 specific and inter-related recommendations for reform.

SUMMARY OF PROPOSALS

Shape of the new law

10. A comprehensive and comprehensible new law should be drafted from scratch, replacing the multitude of current powers and providing for clear limits and safeguards on any intrusive power that it may be necessary for public authorities to use.[1]

11. The definitions of content and of communications data should be reviewed, clarified and brought up to date.[2]

Capabilities

12. The power to require service providers to ***retain communications data*** for a period of time should continue to exist, consistently with the requirements of the ECHR and of EU law.[3]

1 Recommendations 1-9, 14.3-14.7 below.
2 Recommendation 12, 14.10-14.12 below.
3 Recommendations 13-14, 14.14-14.22 below.

13. In relation to the subject-matter of the ***2012 Communications Data Bill***:

    a. The provisions for ***IP resolution*** in the Counter Terrorism and Security Act 2015 are useful and should be kept in force.[4]

    b. The compulsory retention of records of user interaction with the internet (***web logs*** or similar) would be useful for attributing communications to individual devices, identifying use of communications sites and gathering intelligence or evidence on web browsing activity. But if any proposal is to be brought forward, a detailed operational case needs to be made out, and a rigorous assessment conducted of the lawfulness, likely effectiveness, intrusiveness and cost of requiring such data to be retained.[5]

    c. There should be no question of progressing proposals for the compulsory ***retention of third party data*** before a compelling operational case for it has been made out (as it has not been to date) and the legal and technical issues have been fully bottomed out.[6]

14. The capability of the security and intelligence agencies to practise ***bulk collection*** of intercepted material and associated data should be retained (subject to rulings of the courts),[7] but used only subject to ***strict additional safeguards*** concerning:

    a. judicial authorisation by ISIC;[8]

    b. a tighter definition of the purposes for which it is sought, defined by operations or mission purposes;[9]

    c. targeting at the communications of persons believed to be outside the UK at the time of those communications;[10] and

    d. the need for a specific interception warrant to be judicially authorised if the applicant wishes to look at the communication of a person believed to be within the UK.[11]

15. There should be a ***new form of bulk warrant***, the bulk communications data warrant, which would be limited to the acquisition of communications data and could thus be a proportionate option in certain cases.[12]

4 Recommendation 14 below.
5 Recommendations 15-17, 14.32-14.36 below.
6 Recommendation 18, 14.37-14.38 below.
7 Recommendation 19, 14.39-14.45 below.
8 Recommendations 22, 45-48, 14.47-14.57 below.
9 Recommendation 43, 14.75 below.
10 Recommendation 44, 14.76-14.77 below.
11 Recommendation 79, 14.89 below.
12 Recommendation 42(b) and 44, 14.73 and 14.77 below.

Warrants for interception

16. All warrants should be ***judicially authorised*** by a Judicial Commissioner at a new body: the Independent Surveillance and Intelligence Commission (ISIC).[13]

17. Where a warrant is said to be required in the interests of a ***national security purpose that relates to the defence and/or foreign policy*** of the UK, the Secretary of State should have the power so to certify (and, in the case of a bulk warrant, to certify that the warrant is required for the operation(s) or mission purpose(s) identified). The Judicial Commissioner, in determining whether to issue the warrant, should have the power to depart from that certificate only on the basis of the principles applicable in judicial review.[14]

18. ***Specific interception warrants*** may be targeted not only on persons or premises but (like the existing thematic warrants) on operations. That is subject to the additional protection that, save where ordered by the Judicial Commissioner, the addition of persons and premises to the schedule of the warrant must be specifically authorised by a Judicial Commissioner.[15]

19. The warrantry procedure should be ***streamlined*** by providing for:

    a. Serious crime warrants, like national security warrants, to be of six months' duration;[16]

    b. Renewals to take effect from the expiry of the original warrant;[17]

    c. Combined warrants for interception, intrusive surveillance and/or property interference, so long as the conditions for each type of warrant are individually satisfied.[18]

20. Pending a longer-term and more satisfactory solution, the extraterritorial effect in DRIPA s4 should be maintained.[19]

Authorisation for acquisition of communications data

21. Designated persons (DPs) (including in the security and intelligence agencies) should be required by statute to be independent from the operations and investigations in relation to which they consider whether to grant an authorisation.[20]

22. Single Points of Contact (SPoCs) should be provided for in statute.[21]

---

13 Recommendation 22, 14.47-14.57 below.
14 Recommendations 30 and 46, 14.64-14.66 below.
15 Recommendations 26-38, 14.60-14.70 below.
16 Recommendation 37, 14.69 below.
17 Recommendation 38, 14.70 below.
18 Recommendation 39, 14.71 below.
19 Recommendations 24-25, 14.58-14.59 below.
20 Recommendation 58, 14.80 below.
21 Recommendation 62, 14.78 below.

23. The SPoC function for all ***minor users*** of communications data should in future be compulsorily performed by an independent SPoC at the National Anti-Fraud Network (NAFN).[22]

24. Now that all local authority requests for communications data must be submitted to independent SPoCs at NAFN and approved by a designated person of appropriate seniority, the additional requirement of ***approval by a magistrate or sheriff should be abandoned***.[23]

25. The DP of any public authority which seeks communications data for the purpose of determining ***matters that are privileged or confidential*** must either refuse the request or refer it to ISIC for determination by a Judicial Commissioner.[24]

26. Where a request is not directed to such a purpose but relates to ***persons who handle privileged or confidential information*** (doctors, lawyers, journalists, MPs etc.), special considerations and arrangements should be in place, and the authorisation if granted should be flagged for the attention of ISIC.[25]

27. Where a ***novel or contentious request*** is made for communications data, the requesting public authority on the advice of the DP should refer the matter to ISIC for a Judicial Commissioner to decide whether to authorise the request.[26]

Oversight and review

28. The ***Independent Surveillance and Intelligence Commission*** (ISIC) should replace the offices of the three current Commissioners.[27]

29. ISIC should take over the ***intelligence oversight*** functions of the ISCommr, the existing ***auditing*** functions of its predecessor Commissioners, and ***additional functions*** relating in particular to the acquisition and use of communications data, the use of open-source intelligence and the sharing and transfer of intercepted material and data.[28]

30. Through its Judicial Commissioners, who should be serving or retired senior judges, ISIC should also take over the ***judicial authorisation*** of all warrants and of certain categories of requests for communications data, in addition to the approval functions currently exercised by the OSC in relation to other forms of surveillance and the ability to issue guidance.[29]

22 Recommendation 65, 14.84 below.
23 Recommendation 66, 14.82-14.83 below.
24 Recommendation 68, 14.85(a) below.
25 Recommendation 67, 14.85(b) below.
26 Recommendations 70-71, 14.86 below.
27 Recommendations 82-112, 14.94-14.100 below.
28 Recommendations 89-97, 14.95-14.96 below.
29 Recommendations 84-88, 14.95 below.

31. ISIC, on its own initiative or at the suggestion of a public authority or CSP, should have additional powers to notify subjects of their right to lodge an application to the IPT.[30]

32. ISIC should be public-facing, transparent, accessible to media and willing to draw on expertise from different disciplines.

33. The ***Investigatory Powers Tribunal*** (IPT) should have an expanded jurisdiction and the capacity to make declarations of incompatibility; and its rulings should be subject to appeal on points of law.[31]

Transparency

34. Whilst the operation of covert powers is and must remain secret, public authorities, ISIC and the IPT should all be as open as possible in their work. Intrusive capabilities should be avowed. Public authorities should consider how they can better inform Parliament and the public about why they need their powers, how they interpret those powers, the broad way in which those powers are used and why additional capabilities may be required.[32]

CONCLUSION

35. RIPA, obscure since its inception, has been patched up so many times as to make it incomprehensible to all but a tiny band of initiates. A multitude of alternative powers, some of them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and – in the long run – intolerable.

36. Parliament provided the Review with a broad canvas,[33] which I have done my best to cover. The recommendations in Chapter 15 aim to provide a clear, coherent and accessible scheme, adapted to the world of internet-based communications and encryption, in which:

    a. public authorities have limited powers, but are not shut out from places where they need access to keep the public safe;

    b. procedures are streamlined, notably in relation to warrants and the authorisation of local authority requests for communications data;

    c. safeguards are enhanced, notably by:

        i. the authorisation of warrants by senior judges;

        ii. additional protections relating to the collection and use of communications by the security and intelligence agencies in bulk;

30 Recommendation 99, 14.103-14.104 below.
31 Recommendations 99 and 113-117, 14.101-14.108 below.
32 Recommendations 9 and 121-124, 14.7 and 14.110-14.111 below.
33 1.2 below.

iii. greater supervision of the collection of communications data, including judicial authorisation where privileged and confidential material is in issue or novel and contentious requests are made;

iv. improved supervision of the use of communications data, including in conjunction with other datasets and open-source intelligence; and

v. a new, powerful, visible and accountable intelligence and surveillance auditor and regulator.

37. My aim has been to build on the best features of the current regime and to learn from the practice of other countries. The resulting framework aims not only to satisfy the majority who broadly accept current levels of investigatory activity and supervision,[34] but to help build trust among sceptics both in the UK and abroad.

38. The opportunity now exists to take a system characterised by confusion, suspicion and incessant legal challenge, and transform it into a world-class framework for the regulation of strong and vital powers. I hope that opportunity will be taken.

[34] 2.27 and 2.34 below.

DETAILED CONTENTS

PART I: BACKGROUND

1. INTRODUCTION **15**

Genesis of the Review **15**

Context of the Review **15**

Scope of the Review **19**

Working methods **22**

Terminology **23**

Treatment of classified material **23**

2. PRIVACY **25**

Introduction **25**

The evolution of privacy **25**

Perspectives on privacy **26**

Why is privacy important? **27**

Privacy: a qualified right **28**

The position of the UK **29**

Modern attitudes to privacy **32**

The Snowden effect **34**

Is privacy dead? **36**

3. THREATS **39**

Introduction **39**

The threat in perspective **39**

The importance of good order **40**

National security threats **41**

Crime and public safety **44**

Conclusion **47**

4. TECHNOLOGY **49**

Introduction **49**

Changing methods of communication **49**

Global nature of the internet **51**

Fragmentation of providers 52
Difficulties in attributing communications 52
New sources of data 54
Geographical changes 59
Encryption 60
The dark net 65
Anonymity and anti-surveillance tools 66
Decentralised networks 67
New capabilities 68

PART II: CURRENT POSITION

5. LEGAL CONSTRAINTS 71
The common law 71
The European Convention on Human Rights 73
The law of the European Union 84
International Law 92

6. POWERS AND SAFEGUARDS 95
Key concepts 95
Powers outside RIPA 97
Other intrusive capabilities 100
RIPA powers 103
RIPA safeguards 113
Data Sharing 115
Oversight 119

7. PRACTICE 124
Sources and scope 124
The Snowden Documents 124
Interception 126
Communications data 133
Computer network exploitation 137
Intelligence sharing 138
Bulk Personal Datasets 139
The Management of Relationships with CSPs 139

8. COMPARISONS 141
Other forms of surveillance 141
International Comparisons 148
Private sector activity 154

PART III: PERSPECTIVES AND VISIONS

9. LAW ENFORCEMENT 166
Scope and sources 166
Summary of requirements 167
Utility of intercept and communications data 168
Capabilities: interception 172
Capabilities: communications data 173
Minor users 183
Oversight 188

10. INTELLIGENCE 190
Scope and sources 190
The Agencies 192
Summary of requirements 193
Agency capabilities 194

11. SERVICE PROVIDERS 203
Scope and sources 203
The importance of trust 203
International enforcement 204
Views of service providers 205

12. CIVIL SOCIETY 213
Sources and scope 213
Transparency 213
Coherence and clarity 218
Scope of investigatory powers 223
Increase scrutiny and safeguards 227

Improve oversight 235
Future-proofing 242

PART IV: CHARTING THE FUTURE

13. PRINCIPLES 245
A question of trust 245
First principle: minimise no-go areas 247
Second principle: limited powers 248
Third principle: rights compliance 251
Fourth principle: clarity and transparency 252
Fifth principle: a unified approach 253
Recommendations – the objective 255

14. EXPLANATIONS 257
INTRODUCTION 257
GENERAL (Recommendations 1-12) 258
CAPABILITIES (Recommendations 13-19) 260
INTERCEPTION AND ACQUISITION OF DATA (Recommendations 20-71) 270
USE OF INTERCEPTED MATERIAL AND DATA (Recommendations 72-81) 279
OVERSIGHT AND REVIEW (Recommendations 82-121) 280
TRANSPARENCY (Recommendations 121-124) 284

15. RECOMMENDATIONS 285
GENERAL 285
CAPABILITIES 287
INTERCEPTION AND ACQUISITION OF DATA 288
USE OF INTERCEPTED MATERIAL AND DATA 297
OVERSIGHT AND REVIEW 299
TRANSPARENCY 306

PART I: BACKGROUND

Part I of the Report (BACKGROUND) establishes the context for the Review, explores the central concept of privacy and considers both current and future threats to the UK and the challenges of changing technology.

- **Chapter 1 (INTRODUCTION)** sets out the scope, aims and methodology of the Review.

- **Chapter 2 (PRIVACY)** looks at the importance of privacy for individual, social and political life. It charts attitudes to privacy and surveillance as they have evolved over time and as they have recently been captured in court judgments and in survey evidence from the UK and elsewhere.

- **Chapter 3 (THREATS)** looks at the importance of security for individual, social and political life. It assesses the threat to the UK in terms of both national security and crime, and puts it into a long-term perspective.

- **Chapter 4 (TECHNOLOGY)** explains the basic technology that underlies the debate, from changing methods of communication and new capabilities to encryption, anti-surveillance tools and the dark net.

1. INTRODUCTION

Genesis of the Review

1.1. The Data Retention and Investigatory Powers Act 2014 **[DRIPA 2014]** completed its parliamentary passage in just four days, receiving Royal Assent on 17 July 2014. Emergency legislation was said to be needed in order to ensure that UK law enforcement and security and intelligence agencies could maintain their ability to access the telecommunications data they need to investigate criminal activity and protect the public. As part of the political agreement that secured cross-party support for the Bill, the Home Secretary was required (by DRIPA 2014 s7) to "*appoint the independent reviewer of terrorism legislation to review the operation and regulation of investigatory powers*". This Report is the outcome of that Review.

1.2. I am required to consider, in particular:

> "(a) current and future threats to the United Kingdom;
>
> (b) the capabilities needed to combat those threats;
>
> (c) safeguards to protect privacy;
>
> (d) the challenges of changing technologies;
>
> (e) issues relating to transparency and oversight;
>
> (f) the effectiveness of existing legislation (including its proportionality) and the case for new or amending legislation."[1]

1.3. The Review was to be completed so far as reasonably practicable by 1 May 2015, and a report sent to the Prime Minister as soon as reasonably practicable after completion.[2] This report is up to date to 1 May 2015, and was sent to the Prime Minister on 6 May 2015. On receipt, the Prime Minister is obliged to lay a copy of the Report before Parliament, together with a statement as to whether any matter had been excluded from it on the basis that it seemed to him to be "*contrary to the public interest or prejudicial to national security*".[3]

Context of the Review

Data retention and extraterritoriality

1.4. The two matters said to justify the emergency passage of DRIPA 2014 were:

(a) the April 2014 ruling of the Grand Chamber of the Court of Justice of the European Union **[CJEU]** in the *Digital Rights Ireland* case,[4] **[Digital Rights Ireland]**, declaring invalid the ***EU Data Retention Directive***[5] which provided

---

1 DRIPA 2014, s7(2).
2 DRIPA 2014, s7(3)(4).
3 DRIPA 2014, s7(5)(6).
4 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* and *Seitlinger and others*, EU:C:2014:238.
5 Directive 2006/24/EC: **[EU Data Retention Directive]**.

the legal basis for UK Regulations requiring service providers[6] to retain communications data for law enforcement purposes for a specified period;[7] and

(b) the need to put beyond doubt the ***extraterritorial effect*** of warrants, authorisations and requirements relating to interception and communications data, so that they could for example be served on overseas service providers.

These matters were addressed in DRIPA 2014 ss1 and 4, respectively. Other technical and definitional changes were made by the Act. According to its Explanatory Memorandum, the purpose of DRIPA 2014 was "*not ... to enhance data retention powers*", but rather to preserve pre-existing capabilities.[8]

1.5. In recognition of the very short time available for debate, DRIPA 2014 contains a "*sunset clause"* which provides for its operative provisions to expire at the end of 2016.[9] Ministers and Shadow Ministers expressed the hope that the present Report will assist Parliament's consideration of whether the data retention and extraterritoriality powers contained in DRIPA 2014 should be renewed beyond that date.[10]

The broader context

1.6. But as the wide terms of s7 confirm, the scope of this Review extends well beyond the provisions of DRIPA 2014. The setting up of the Review reflects a broader political context, including:

(a) what law enforcement and intelligence bodies had identified as their ***reduced coverage of electronic communications***, as a consequence of:

- the long-term shift from telephone communications via UK service providers towards internet-based communications through overseas (especially US) service providers; and

- other technological changes, including the growth of secure encryption for internet communications;[11]

6 For ease of reference, the term "*service providers*" is used to refer to: (1) companies which offer communications services (**[CSPs]** properly so called), such as BT and Vodafone, (2) companies providing internet access (commonly referred to as Internet Service Providers **[ISPs]**), such as AOL, Virgin Media and Sky (collectively, technical readers will know these two categories as the four lower levels of the OSI 7-layer model), and (3) companies which operate "*over the top*" **[OTT]** of an internet connection (commonly called OTT providers or applications services providers), such as Facebook and Twitter. Some CSPs are also ISPs. Some companies offer communications services, internet access and OTT services (e.g. BT TV, over its own internet service). Reference is made to the individual category of service provider where necessary. The term CSP is used when referring to both CSPs and ISPs.

7 The Data Retention (EC Directive) Regulations SI 2009/859, which were adopted pursuant to the European Communities Act 1972 **[ECA 1972]** s2(2). Regulations under the ECA 1972 depend upon the existence of a valid EU instrument.

8 Explanatory Memorandum, para 32.

9 DRIPA 2014 s8.

10 Hansard, HC Debs, 15 July 2014, Col 714 (Theresa May) and Col 723 (Yvette Cooper).

11 See further, 4.41-4.65 below.

(b) the ***Communications Data Bill*** of 2012, which sought to remedy gaps in that coverage in a number of ways (some of which had been prefigured under the previous Government). It was considered in draft by two parliamentary committees, but never introduced to Parliament as a consequence of disagreements within the Coalition;

(c) the ***publication since 2013 of a selection of documents***, removed without authorisation from the US National Security Agency **[NSA]** by the contractor Edward Snowden and purporting to describe various capabilities of the NSA and other agencies, including the UK's Government Communications Headquarters **[GCHQ]**, **[the Snowden Documents]**;[12] and

(d) the various ***consequences of publication*** of the Snowden Documents, including:

- disquiet and suspicion among sections of the public in the UK and other countries, prompted in particular by allegations of bulk collection and analysis of data on a previously unreported scale;
- a new emphasis by service providers on customer privacy, reflected in a quickening of the trend towards universal encryption and a reduction in voluntary cooperation with foreign governments;
- pleas from law enforcement and security and intelligence agencies for better cooperation from overseas service providers, and better means of enforcement against them; and
- unprecedented levels of activity from the UK's supervision mechanisms, in particular the Investigatory Powers Tribunal **[IPT]**, Interception of Communications Commissioner's Office **[IOCCO]** and Intelligence and Security Committee of Parliament **[ISC]**, each of which has examined and reported on allegations arising out of the Snowden Documents.

1.7. The debate is thus a double-jointed one, featuring arguments for more and for less capability, for more safeguards and for the removal of limitations that serve no useful purpose. If it is at times bitterly contested, that is because both sides (with unquestionable sincerity) see their position as under threat:

(a) Privacy advocates emphasise the growing volume of electronic communications, as well as their quality, and extended techniques for the gathering and analysis of them, as lives are increasingly lived online. They campaign for reduced powers, or at any rate enhanced safeguards, to protect the individual from the spectre of a surveillance state.

[12] A catalogue of the Snowden Documents placed in the public domain is maintained by the Lawfare Institute: http://www.lawfareblog.com/catalog-of-the-snowden-revelations/. See also the Snowden Digital Surveillance Archive: https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi and The Electronic Frontier Foundation: https://www.eff.org/nsa-spying/nsadocs.

(b) The authorities see a decline in the proportion of electronic communications which they have the ability to access or to make use of, fear the emergence of channels of communication that cannot be monitored, and seek to redress the balance with new powers in the interests of national security and the prevention and detection of crime.

Each sees a future in which they lose control. Privacy advocates look at a world in which ever more data is produced, aggregated and mined. The authorities fear developments such as universal default encryption, peer-to-peer networks and the dark net.

The effect of Snowden

1.8. Each of the rival camps is well-entrenched: the Communications Data Bill was being proposed, and caricatured as a "*snoopers' charter*", before anyone had heard of Edward Snowden. But the Snowden Documents have transformed the position in a number of ways.

(a) They have provided material for debate: though the UK Government retains its strict policy of "*neither confirm nor deny*" **[NCND]**,[13] some capabilities have been admitted (notably PRISM, after its acknowledgment by the US Government, and computer network exploitation **[CNE]**) and the IPT in particular has been prepared to review the lawfulness of other programmes (such as TEMPORA) on the basis of assumed facts.

(b) For privacy advocates, the Snowden Documents have caused them to believe that investigatory powers are used more widely even than they had suspected, and provided a nucleus for wide-ranging litigation.[14]

(c) The opening up of the debate has however come at a cost to national security: the effect of the Snowden Documents on the behaviour of some service providers and terrorists alike has, for the authorities, accentuated the problem of reduced coverage and rendered more acute the need for a remedy.

The international dimension

1.9. There is some evidence that reaction to the Snowden Documents was less marked, and less negative, in the UK than in some other countries.[15] But to approach the debate as though domestic considerations are all that matter is not realistic, for at least four reasons:

(a) International travel, the global nature of the internet and the ability to tap international cables means that the use of investigatory powers by UK authorities inevitably impacts upon persons who are neither British citizens nor present in the UK.

---

13 Though see *Belhadj and others v Security Service and other* (Case no. IPT/13132-9/H) **[Belhadj IPT Case]**, judgment of 29 April 2015.

14 See further 5.35-5.54 below.

15 See 2.25-2.35 below.

(b) The safeguards on the use of those powers must be sufficiently strong not only to satisfy public opinion in the UK, but to persuade governments and overseas service providers (including particularly in the USA) that they can and should cooperate with requests for information.

(c) For as long as the UK accepts the jurisdiction of the European Court of Human Rights **[ECtHR]** and CJEU, its law must conform to the principles of their jurisprudence, with its strong emphasis on the protection of private communications, as well as to the constraints of international law.

(d) Whatever solution the UK arrives at may well be influential in other countries. Nothing should be proposed for the UK that would not be accepted if it were adopted by other democratic nations.

Scope of the Review

Definition of investigatory powers

1.10. The "*investigatory powers*" that I am required to review are not defined in DRIPA 2014, nor even in the central piece of legislation in this area: the Regulation of Investigatory Powers Act 2000 **[RIPA]**. It might have been legitimate to understand the phrase as encompassing the full range of such powers, including directed and intrusive surveillance (tailing, bugging), property interference and the use of covert human intelligence sources **[CHIS]**. The concept might even be extended further, to cover surveillance cameras and DNA databases.

1.11. I have however approached the task with regard to my initial Terms of Reference, issued in July 2014, which define the objective of the Review as being

> "[t]o review the use of legislation governing the use of communications data and interception ...",

with regard among other things to "*the effectiveness of current statutory oversight arrangements*".[16] The Security Minister confirmed during the passage of the Bill that this was the intended scope of the Review.[17] Interception and communications data are governed by RIPA Part I; RIPA Part IV covers codes of practice and scrutiny by Commissioners and by the IPT. Those are the subjects I have covered in this Review, though by reference also to statutes other than RIPA, and with an eye to the comparisons presented by other types of surveillance and spying powers, particularly when they are used for similar purposes, as for example CNE may be. Some of my recommendations, if adopted, will affect such powers.

16 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/330749/Review_of_Communications_Data_and_Interception_Powers_Terms_of_Reference.pdf.

17 Hansard HC Debs 15 July 2014 cols 804, 806.

Objectives of this Report

1.12. Even so limited, DRIPA 2014 s7 presents me with a very broad canvas. In seeking to cover it, my objectives have been two-fold:

(a) to ***inform the public and parliamentary debate*** by providing the legal, technological and operational context, and by seeking to encapsulate the views of the main stakeholders; and

(b) to ***offer my own proposals for change***, based on all the evidence I have heard and read.

Though I seek to place the debate in a legal context, it is not part of my role to offer a legal opinion (for example, as to whether the bulk collection of data as practised by GCHQ is proportionate). A number of such questions are currently before the courts, which have the benefit of structured and opposing legal submissions and (in the case of the IPT) the facility to examine highly secret evidence, and which are the only bodies that can authoritatively determine them.

1.13. Deciding the content of the law in this area is for Parliament, subject only to any external legal constraints; and there are wide issues of principle on which the views of one individual (or even one committee) could never aspire to be determinative.[18] But I am invited to opine on a variety of topics, some of them quite technical in nature, and hope that by basing my conclusions where possible on evidence, MPs and others will at least be in a position to judge whether my recommendations are worthy of being followed.

Not limited to terrorism

1.14. This Review overlaps only slightly with my work as independent reviewer of terrorism legislation.[19] In that (part-time) capacity, I report regularly to Ministers and to Parliament on the operation of laws directed specifically to counter-terrorism, but not on laws relating to investigatory powers, which are within the competence of others.[20] The subject matter of this one-off Review is therefore quite distinct from the normal work of the independent reviewer.

1.15. I would emphasise that:

(a) Investigatory powers vary greatly in their impact. Broad powers of bulk collection are used by GCHQ to identify threats to national security from vast quantities of data. But highly targeted communications data requests are used

---

18 See e.g. the issue of whether the retention by service providers of data capable of revealing web browsing history constitutes an acceptable intrusion into privacy, which the Joint Committee on the Draft Communications Data Bill **[JCDCDB]** after its own thorough investigation felt compelled to leave to Parliament: Report of the JCDCDB, HL Paper 79 HC 479, (December 2012) **[JCDCDB Report]**, para 294.

19 I remain a Q.C. (self-employed barrister) in independent practice. Full details of the role of independent reviewer, and of the reports I have produced in the course of it, are on my website: https://terrorismlegislationreviewer.independent.gov.uk/.

20 In particular, IOCCO. Other forms of surveillance are reported upon by the Intelligence Services Commissioner **[ISCommr]** and by the Office of Surveillance Commissioners **[OSC]**.

for such relatively straightforward tasks as tracing the maker of a 999 (emergency) call, or a "*reverse look-up*" to identify any mobile phones registered to a particular postal address.

(b) Some powers are used (and were always intended to be used) by a wide range of public authorities, from the National Crime Agency **[NCA]** to local authorities, and for a host of purposes including murder investigations, the tracing of missing persons, the investigation of organised crime, the detection of cyber crime (including child sexual exploitation and online fraud) and the enforcement of trading standards.

1.16. It would be unfortunate if my association with the review of terrorism laws were to fuel the common misconception that investigatory powers are designed solely or even principally to fight terrorism. They have a vital part to play in that fight, as this Report will set out. But they are properly and productively used both in a broader national security context (e.g. counter-espionage, counter-proliferation) and in combating a wide range of other crimes, most of them more prevalent than terrorism and some of them just as capable of destroying lives.

Structure of this Report

1.17. The structure of this Report should be evident from the Contents. In summary:

(a) Part I introduces the task, explores the central concept of privacy and discharges my statutory function of reviewing "*current and future threats to the United Kingdom*" and "*the challenges of changing technologies*".[21]

(b) Part II explains the current position, touching on legal constraints before summarising existing powers and how they are used by the authorities. It also seeks to provide some alternative reference points by looking at other types of surveillance by public authorities, the laws of other countries and the use of communications data by private companies.

(c) Part III seeks to summarise the views expressed to the Review by the four main groups which submitted evidence to the Review: law enforcement, intelligence, service providers and civil society.

(d) Part IV explains and sets out my recommendations for change. Drawing on previous parts of the Report, it incorporates my conclusions on "*the capabilities needed to combat those threats*", "*safeguards to protect privacy*", "*issues relating to transparency and oversight*" and "*the effectiveness of existing legislation (including its proportionality) and the case for new or amending legislation*".[22]

21 DRIPA 2014, s7(a)(d).
22 DRIPA 2014, s7(b)(c)(e)(f).

Other reviews

1.18. The initial terms of reference state that my Review will take account of:

> "the findings of the [JCDCDB], RUSI Review, the ISC Privacy and Security Inquiry and administrative and resource impacts".

1.19. Of the three bodies there mentioned:

(a) The JCDCDB reported on 11 December 2012, in the ***JCDCBC Report***: I refer its findings in Chapters 4, 8, 9, 14 and 15, below.

(b) The ISC produced its report **[ISC Privacy and Security Report]** on 12 March 2015.[23] In keeping with the functions of the ISC, that report is limited to the activities of the security and intelligence agencies; but it made some far-reaching recommendations, including for the drafting of a bespoke new law to cover all intelligence agency activity.

(c) The Royal United Services Institute **[RUSI]** Independent Surveillance Review **[the RUSI Review]** announced by the Deputy Prime Minister on 4th March 2014, has not yet reported.

According to the same terms of reference, this Report is to mark the end of the first phase of a Review that will be carried on by a Joint Committee to be established in the next Parliament. I have no doubt that the RUSI Review, and all other relevant material, will be given due weight during the second phase.

Working methods

1.20. I issued a formal call for evidence in July 2014, on my website and via twitter, which was supplemented by a number of specific requests and attracted written submissions (sometimes on a repeated basis) from 67 individuals, NGOs, service providers, individuals, regulators and public authorities. Most in the latter category are classified because of operational sensitivities; but the submissions that I have consent to publish may be found on my website.[24] Almost without exception I have found them useful, informative and thought-provoking.

1.21. I followed up many of the submissions orally and have held meetings with a wide range of interlocutors in the UK.[25] I have benefited from the wide range of expertise presented at Wilton Park meetings in October and November 2014, which provided a unique opportunity for dialogue between people with very different perspectives, and from conferences organised by the Bingham Centre for the Rule of Law and by JUSTICE. I made productive trips to Berlin, San Francisco and Silicon Valley, Washington DC and Ottawa, all in December 2014, and to Brussels in January 2015.

---

23 *Privacy and Security: A modern and transparent legal framework*, HC 1075, (March 2015).

24 https://terrorismlegislationreviewer.independent.gov.uk/.

25 In keeping with the mode of operation of the independent reviewer of terrorism legislation, and in order to achieve maximum frankness from those to whom I spoke, those meetings were confidential and not formally minuted. They included several meetings with and fact-finding visits to the Security Service **[MI5],** the Secret Intelligence Services **[MI6]** and GCHQ.

Full lists of all those who made written submissions to the Review, and of the organisations (and in some cases individuals) with whom I have spoken, are at Annex 3 and Annex 4 to this Report.

1.22. In addition, the ISC shared with me the entirety of the extensive closed evidence that it took as part of its own Privacy and Security Review, and I have seen the confidential parts of the ISC's report as well as of the reports of IOCCO and the ISCommr. Much highly classified material was volunteered to me, and nothing that I asked to see, however sensitive or secret, was withheld from me.

1.23. I was fortunate to recruit to the Review team two barristers (Tim Johnston and Jennifer MacLeod), a solicitor (Rose Stringer) and a former civil servant (Robert Raine CBE), each of whom, despite other commitments, has given substantial time and effort to the Review, greatly extending its reach and helping to ensure its quality. Dr Bob Nowill agreed to act as technical consultant: he has explained much and saved me from a number of errors. Commissioners, judges, academics, lawyers, non-governmental organisations **[NGOs]**, technology experts, retired civil servants and others from across the world have been generous with their help: they have done much to challenge and influence my views. Eric King, Tom Hickman, Ben Jaffey and Jo Cavan each commented on one or more draft Chapters dealing with technology, law and practice. None of the above should be associated with any of the views expressed in this Report, which (like any factual errors) are my responsibility alone.

Terminology

1.24. Lists of the acronyms and definitions used in this Report are at Annex 1 and Annex 2 respectively.

Treatment of classified material

1.25 It is my practice when reviewing the terrorism laws to produce a single, open report which can be shared with Parliament and public without the need for redactions. I have followed the same approach in this report. My aim was to ensure that the Prime Minister would not be called upon to use his power of exclusion under DRIPA s7. To that end I have shared parts of my draft report with the Government in advance, for the purpose of ensuring that national security-sensitive passages could be identified and, by negotiation or agreement, rendered acceptable for public release.

1.26 In a few respects (e.g. the bulk collection case studies at Annex 9), this Report contains material that security and intelligence agencies have not previously put into the public domain. But it has not been possible to deal in the pages of this Report with everything that is relevant to the Review.[26]

1.27 I have emphasised in my Recommendations the importance of transparency, of public avowal, and of backing all capabilities with accessible and foreseeable legal provisions.[27] More broadly, my conclusions have been arrived at on the basis of all

[26] This will not be surprising to any reader of the ISC's Privacy and Security Report: the existence of classified material relevant to its subject and to mine is indicated by the frequent use of asterisks.

[27] See in particular Recommendations 3-5, 8-10 and 121-124.

the information I have myself received: both that which can be disclosed and that which cannot. But it is only fair to point out that (as would no doubt be expected) there are matters relevant to this Review that cannot be referred to in public and that I have therefore not referred to at all.

2. PRIVACY

Introduction

2.1. The exercise of investigatory powers impinges on a variety of human rights and interests, including (as will be seen) freedom of expression, freedom of assembly and the peaceful enjoyment of property. At the root of them are concepts which have been described in international human rights instruments as "*the right to respect for … private … life, home and communications*" and "*the right to protection of personal data*".[1] The catch-all word "*privacy"* is often used, and will be used here, as an imprecise but useful shorthand for such concepts.

2.2. The UK public and courts are sometimes said to be less protective of privacy than their counterparts elsewhere: a proposition that I examine at 2.26-2.35 below. But as has been pertinently remarked:

> "A public that is unable to understand why privacy is important – or which lacks the conceptual tools necessary to engage in meaningful debates about its value – is likely to be particularly susceptible to arguments that privacy should be curtailed."[2]

This Chapter seeks to look under the surface of what we call privacy, in order better to understand the reasons why investigatory powers need to be limited and to inform the debate on the form that such limitations should take.

The evolution of privacy

2.3. It has been claimed that privacy is a "*modern*" concept, a "*luxury of civilisation*", unknown (and unsought) in "*primitive or barbarous*" societies.[3] But ideas of privacy, including the relative freedom of the home from intrusion, are set out in the Code of Hammurabi of Ancient Babylonia, the laws of Ancient Greece and Rome and of Ancient China.[4] References are found to privacy in a range of religious texts, including the Bible, the Koran, and Jewish law.[5] Anthropologists have suggested that the need for privacy, while sensitive to cultural factors, is not limited to certain cultures. Rather, most societies regard some areas of human activity as being private, even if there are

---

1 European Union Charter of Fundamental Rights **[EU Charter]**, Articles 7 and 8, a formulation updated from that in the European Convention of Human Rights **[ECHR]**, Article 8, which is "*the right to respect for … private … life ... home and correspondence*". On these instruments, see further 5.12-5.23 and 5.57-5.58 below.

2 B. J. Goold, "Surveillance and the Political Value of Privacy"*,* Amsterdam Law Forum (2009) ("Goold").

3 See EL. Godkin*,* "The Rights of the Citizen: To His Reputation"*,* (1980) 8 Scribner's Magazine 58, p. 65; and R. Posner, "An Economic Theory of Privacy", (1978) AEI Journal on Government and Society, 19, p. 20.

4 See A. Rengel, *Privacy in the 21st Century,* 2013, ("Rengel"), p. 29; Samuel Dash, *The Intruders: Unreasonable Searches and Seizures from King John to John Ashcroft*, 2004 ("Dash"), pp. 8-10.

5 See Rengel, p 29, and Dash, pp. 8-10.

differences concerning what or how much is private;[6] and humans need privacy to develop into adults, court, mate and rear offspring.[7]

Perspectives on privacy

2.4. The elements of privacy are strongly interlinked, and subject to no academic consensus. In the words of one scholar, privacy is "*a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all*".[8] It may however be useful to refer to a number of formulations that are of relevance to the subject-matter of this Review.

2.5. A classic formulation of privacy is ***the right to be let alone***,[9] once proclaimed to be the "*most comprehensive of rights and the right most valued by civilized men".*[10] This right has been associated with human dignity,[11] with the notion of the *"inviolate personality*" and with the need for beliefs, thoughts, emotions and sensations to be protected from unwanted prying.[12]

2.6. The same principle can be expressed in terms of a positive ***right to conceal or hide information about ourselves***. The idea of a "*sphere*" or zone in which privacy should be assured can be extended by the idea that we operate in different spheres in different situations: see for example the approach of the Canadian Supreme Court, which has identified three broad types of privacy interest – territorial, personal and informational – in respect of which different expectations and rules may apply.[13]

2.7. Privacy can also be understood in terms of ***control***. Since knowledge is power, the transfer of private information to the state can be seen as a transfer of autonomy and of control. Even if the information is never actually read – for example, an electronic communication which was obtained pursuant to a bulk data collection exercise but not selected for scrutiny – the fact that it could be read may be seen as placing control in the hands of the state. Control may also be transferred when information is given to an online service provider, though with the distinguishing factors that consent is required (nominally, at least) and that service providers, while they may use or sell the data within the limits of their terms and conditions, lack the coercive powers of the state.

---

6 See the discussion in Rengel, p. 28.

7 See Rengel, p. 28 and D. Solove, "Conceptualizing Privacy", (2002) 90 Cal.L.Rev. 10987 ("Solove"). Nagel has argued that it is our desire for privacy that separates us from other animals; T. Nagel, "Concealment and Exposure", (1998) Philosophy & Public Affairs, Vol 27 No 1 pp. 3-30, ("Nagel") p. 18.

8 R. C. Post, "Three Concepts of Privacy", (2001) 89 Geo. L.J. 2087.

9 S. Warren & L. Brandeis, "The Right to Privacy", (1890-1891) 4 Harv. L. Rev. 193, p. 205.

10 Brandeis J dissenting in *Olmstead v United States,* 277 US 438 (1928), p. 478, later upheld by *Katz v United States* 389 US 347 (1967).

11 See E. Bloustein, "Privacy as an Aspect of Dignity: An Answer to Dean Prosser", (1964) 39 NYU L. Rev. 962 ("Bloustein") p. 974.

12 As enumerated by Brandeis J in *Olmstead v US*.

13 *R v Spencer,* [2014] SCC 43 (CanLII), para 35 et seq.

Why is privacy important?

2.8. Intrusions into privacy have been compared, compellingly, to environmental damage: individually their impact may be hard to detect, but their cumulative effect can be very significant.[14] It is all the more important, therefore, to appreciate precisely why privacy matters, and how intrusions into it can damage the ecosystem that privacy helps to support.

2.9. A good start is provided by the recent judicial description of privacy protection as "*a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society".*[15] As that statement implies, the privacy ecosystem has individual, social and political aspects.

2.10. First, privacy ***enables the expression of individuality***. Without privacy, concepts such as identity, dignity, autonomy, independence, imagination and creativity are more difficult to realise and maintain.[16] Privacy allows us to think and create in freedom, to choose how we love and with whom we share: it enables the "*sheer chaotic tropical luxuriance of the inner life*" to flourish.[17] It facilitates an inner sanctum that others must respect. It grants us the freedom to function autonomously, without our every action being observed (or countermanded) by others. Of course, if we choose to express our individuality in criminal or anti-social ways, privacy can facilitate that too.

2.11. Secondly and relatedly, privacy ***facilitates trust, friendship and intimacy***: qualities that allow us to relate freely to each other and that form the essential basis for a diverse and cohesive society.[18] Conversely, surveillance has been shown to lead to self-censorship[19] and the suppression of certain behaviour,[20] though once again, anti-social as well as pro-social behaviour may be suppressed by surveillance.[21]

2.12. Thirdly, privacy is necessary for the ***securing of other human rights***, ranging from the freedom of political expression to the right to a fair trial. Just as democracy is enabled by the privacy of the ballot box, so the expression of dissenting views is enhanced by the ability to put them across anonymously:[22] the ability of a whistleblower to reveal state misconduct and of a journalist to report it requires an assurance that the journalist's sources will not be made known to the state.[23] There

---

14 See J. Angwin, *Dragnet Nation: A quest for privacy, security and freedom in a world of relentless surveillance*, 2014, ("Angwin").

15 *R v Spencer*, para 15, summarising the effect of previous cases in the Supreme Court of Canada.

16 See Solove*,* p. 1145, and C. Fried, "Privacy"*,* (1968) 77 Yale LJ 475, discussing love, friendship and trust.

17 Nagel, p. 4.

18 Goold; R. Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort"*,* (1989) 77 Cal. L. Rev. 957.

19 See J. Kang, "Information Privacy in Cyberspace Transactions"*,* (1998) 50 Stan. L. Rev 1193, p. 1260.

20 A. Oulasvirta et al, "Long-term Effects of Ubiquitous Surveillance in the Home", Ubicomp' 12, 41.

21 To take a practical example, whether a person reports or owns up to scraping another vehicle in a car park might depend on whether the incident is thought to have been recorded by CCTV.

22 This phenomenon long predates the internet age: see for example William Prynne's anti-prelatical pamphlet "*Newes from Ipswich*", issued in 1636 under the name of Matthew White. The use of a pseudonym and false Ipswich imprint (rather like a Tor exit node: 4.67(b) below) were attempts to conceal the origin of a work that it was known the authorities would consider seditious.

23 See further 5.49-51 below.

can be no fairness in litigation involving the state if one party to it has the ability to monitor the privileged communications of the other.[24] Indeed, Lord Neuberger, President of the UK Supreme Court, recently suggested that, "*at least in many cases"* the right to privacy is "*an aspect of freedom of expression"*; as when one wishes to do or say something only privately, it is an interference with expression when one cannot.[25] He noted that this is particularly true of anonymous speech, where an author's article 8 (privacy) rights "*reinforce"* his or her article 10 (expression) rights, both generally and particularly in relation to confidential speech.[26]

2.13. Fourthly, privacy ***empowers the individual against the state***. The state's ability to monitor communications offers opportunities for manipulation or control, for example by the publication of truthful yet embarrassing facts or images intended to discredit or tarnish the citizen; the ability to predict the actions of citizens and to respond to perceived threats to power; the profiling of dissenters or minority groups; and the capacity to control the information received or dispensed by the target.[27] All these practices, described by George Orwell,[28] were known in totalitarian states from Eastern Europe to Iraq, leading to the observation that intrusion on privacy is a "*primary weapon of the tyrant"*.[29] Echoes of such tendencies have also been observed (and commendably brought to light) in the United States of America.[30]

Privacy: a qualified right

2.14. However powerful the need for privacy, it is not (as is, for example, the prohibition against torture) an absolute right. Just as the interests of public safety and law enforcement will sometimes have to give way to the right to privacy, so the right to privacy may need to yield to competing considerations. That is acknowledged in Article 8(2) of the ECHR, which approves interference by public authorities with the right to respect for private life and correspondence in circumstances where that interference is in accordance with the law, necessary and a proportionate method of achieving specified objectives including the interests of national security, the prevention of disorder or crime and the protection of health.[31]

---

24 See further 5.45-48 below.

25 Lord Neuberger at the Hong Kong Foreign Correspondents' Club, "The Third and Fourth Estates: Judges, Journalists and Open Justice"*,* 26 August 2014.

26 Lord Neuberger at 5 RB Conference, "What's in a name? Privacy and anonymous speech on the Internet"*,* 30 September 2014.

27 Frequently cited in this regard is the comment attributed to Cardinal Richelieu: "*Show me six lines written by the most honest man in the world, and I will find enough therein to hang him.*"

28 *Nineteen Eighty-Four*, 1949.

29 Bloustein, p. 974.

30 The Church Committee, a Senate Committee that sat in the mid-1970s, concluded that "*too many people have been spied upon by too many Government agencies and too much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power"*. Reference was made to the careful surveillance of groups deemed dangerous, on the basis of vague standards, and the use of "*unsavoury and vicious tactics"*. Famous examples set out by the Committee include surveillance and thereafter improper pressure being applied to the Women's Liberation Movement and Dr. Martin Luther King (including using information obtained to encourage him to commit suicide, or to destroy his marriage). The Committee also describes the seeking of "*political intelligence*" from wiretapping under President Nixon and others, including Watergate: *Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities*, 94th Congress, 2nd Session, Report No. 94-755, Book IV, pp. 5-13.

31 See further 5.21-5.22 below.

2.15. The state has a duty to keep those within its borders safe from criminality. That duty is generally acknowledged to require some ability to intrude upon private communications. Where communication channels are unwatched by the state, and still more when they are incapable of being watched, criminals can act with impunity. That common-sense observation is reflected in the routine activity theory, a criminological staple which states that the three necessary conditions for most crime are a likely offender, a suitable target and – significantly – the absence of a capable guardian.

2.16. Whether such intrusion is appropriate, and if so to what extent, is a matter of fierce debate: opinions differ, for example, as to whether it is permissible to interrogate the communications of people not for the time being under suspicion, whether communications providers should be obliged to retain data that they do not keep for commercial purposes, and to whom and under what conditions such data should be made available. Those who mistrust the state tend to argue that such powers should not exist at all; others accept the powers but emphasise the need for robust safeguards on their use. The question of trust is thus at the core of the issues to be considered in this Review: a theme to which I return at 13.1-13.6 below.

2.17. But such debates should not be conducted simply on the level of individual versus state. Any intrusion into privacy is liable to have an impact not only on that relationship, but on the individual and social aspects of privacy, as summarised at 2.10-2.12 above. Those aspects, though less tangible, are just as important. If we neglect them, we risk sleepwalking into a world which – though possibly safer – would be indefinably but appreciably poorer.[32]

The position of the UK

Popular views

2.18. There are signs that the UK public is less troubled by surveillance issues than its counterparts in some other countries (2.25-2.35 below); and that the same distinction is apparent in the rulings of its courts (2.22-2.24 below).

2.19. The need to safeguard privacy against intrusion by the UK Government and its security and intelligence agencies is widely appreciated in theory. Indeed to a substantial minority of the population – including many of the campaigners who have contributed to this Review – it is an issue of the highest importance. But for others, it lacks practical resonance. It is easy to see the utility of closed circuit television **[CCTV]** cameras, DNA databases and communications data in solving crimes, identifying terrorists and protecting children from sexual abuse. It is harder to put a concrete value on concepts such as human dignity and the inviolability of the private sphere, particularly in a country which escaped the totalitarian excesses of the 20th century (thanks in part to the successes of its security and intelligence agencies),[33]

---

32 The threat of "*sleepwalking into a surveillance society*" was thought to be a reality by the Information Commissioner, introducing his *Report on the Surveillance Society,* (2006): see "Britain is 'surveillance society'", BBC news website, 2 November 2006: see further 12.32 below.

33 To give two well-known examples from World War II, the Double Cross counter-espionage system operated by MI5; and the successes of the Government Code and Cypher School, the forerunner of

and in which libertarianism remains an insignificant political force. People are concerned or outraged by isolated uses of surveillance powers, especially by police or local authorities;[34] yet on a broader scale, there was a relatively muted reaction to the publication in 2013-14 of secret documents purporting to reveal the aspirations and inner workings of GCHQ and its partners.

2.20. But attitudes vary widely, both between individuals and over time. An alternative strand of strong British opposition to state surveillance over private life may be illustrated by examples from each of the past four centuries:

(a) Viscount Falkland, appointed Secretary of State in 1643, at the height of the English Civil War, could never bring himself to exercise "*the liberty of opening letters upon a suspicion that they might contain matter of dangerous consequence*", finding it (according to one of his close associates) "*such a violation of the law of nature that no qualification by office could justify a single person in the trespass*".[35]

(b) The 18th century jurist William Blackstone characterised eavesdropping as an offence "*against the public health of the nation; a concern of the highest importance*".[36] Celebrated cases of the period declared that there was no power to issue a general warrant for the search of properties, for "*if there was, it would destroy all the comforts of society; for papers are often the dearest property a man can have*".[37]

(c) In the wake of an 1844 parliamentary enquiry into the interception of letters addressed to the Italian patriot Giuseppe Mazzini, the "*secret branch*" of the Post Office (which dealt with foreign letters) and the deciphering office were closed down, with the result that, according to one historian of the period, "*[t]o most intents and purposes, domestic political espionage in Britain stopped shortly after 1848 ... until the story picks up again in the early 1880s*".[38] Patriotic pride in this state of affairs was expressed by Sir Thomas Erskine May, when he wrote in 1863:

> "Men may be without restraints upon their liberty: they may pass to and fro at pleasure but if their steps are tracked by spies and informers, their words noted down for crimination, their associates watched as conspirators – who shall say that they are free? Nothing is more

GCHQ, in cracking the Enigma codes and so, very probably, shortening the war: C. Andrew *The Defence of the Realm: The Authorized History of MI5,* 2010; and R.J. Aldrich, *GCHQ: the Uncensored Story of Britain's Most Secret Intelligence Agency*, 2010.

34 E.g. the revelation that Bob Lambert, an undercover police officer, tasked to infiltrate an environmental protest group, fathered a child by one of the protesters, leading to a settlement of £425,000 from the Metropolitan Police in 2014; see D. Casciani, "The undercover cop, his lover, and their son", BBC website, 24 October 2014.

35 E. Hyde, Earl of Clarendon, *The History of the Rebellion*, written in 1668-70: Oxford World's Classics edn., 2009, pp. 186-187. Falkland was equally resistant to "*the employing of spies, or giving any countenance or entertainment to them*". But the opening of letters continued: "*convinced by the necessity and iniquity of the time that those advantages of information were not to be declined, and were necessary to be practised*", Falkland "*found means to shift it from himself*": *ibid.*

36 Blackstone's Commentaries, Book 4, Chapter XIII, p. 128.

37 *Entick v Carrington* 2 WILS KB 274, 807, pp. 817-818: see further at 5.4-5.8 below.

38 B. Porter, *Plots and paranoia: a history of political espionage in Britain 1790-1988,* 1989, pp. 77-81.

> revolting to Englishmen than the espionage that forms part of the administrative system of continental despotisms. It haunts men like an evil genius, chills their gaiety, restrains their wit, casts a shadow over their friendships, and blights their domestic hearth. The freedom of this country may be measured by its immunity from this baleful agency."[39]

(d) The dystopian society described in George Orwell's book *Nineteen Eighty-Four* was one in which the inhabitants of Oceania live and work in places equipped with two-way "*telescreens*", allowing them be watched at any time, and in which correspondence is routinely opened and read before delivery. The link between surveillance and total state control is a central theme of the novel, which after its publication in 1949 resonated with particular force in the Soviet Union and Communist Eastern Europe. Phrases such as "*Big Brother*" and "*Thought Police*" remain commonplaces to this day in any debate on surveillance and its limits.

2.21. So generalisation is dangerous. Attitudes will be shaped by experience, personal as well as national. That is as it should be: tolerance of the need for surveillance rightly depends both on how useful and on how intrusive it is, as well as on the threat picture and the degree of risk that society, and its individual members, are prepared to tolerate.

Judicial approaches

2.22. Different concepts of privacy are given prominence in different legal systems. Thus, the concept of dignity is said to underlie continental, and particularly German, privacy law, whereas liberty from the state finds more prominence in United States law.[40]

2.23. The UK – so often positioned midway between the norms of the US and continental Europe – is in this respect something of an outlier: privacy protection from state intrusion was given little emphasis by the common law, and has recently been guaranteed largely under the influence of European legal norms.[41]

2.24. Article 8 is now applied domestically under the Human Rights Act 1998 **[HRA 1998]**, as discussed in detail below (5.13-5.14). However, there is still a striking difference in emphasis between UK judges and the European courts as regards the degree of protection to be accorded to privacy. For example:

(a) In a number of cases, unanimous rulings by the highest UK court have been countermanded by unanimous rulings of the ECtHR upholding privacy rights.[42]

---

39 T.E. May, *Constitutional History of England since the Accession of King George III*, vol. 2, 1863, p. 275.

40 See J. Whitman, "Two Western Cultures of Privacy", (2003-2004) 113 Yale LJ 1151.

41 See 5.11 and 5.17 below.

42 *S v United Kingdom* (Application no. 30562/04; judgment of 4 December 2008) (DNA retention: 0-5 in the judicial House of Lords (0-10 if the lower courts are included) then 17-0 in Strasbourg); *Kay v United Kingdom* (Application no. 37341/06; judgment of 21 September 2010) (home repossession: 0-7 then 7-0); *Gillan v United Kingdom* (Application no. 3158/05; judgment of 12 January 2010) (no-suspicion stop and search: 0-5 then 7-0). A further case (*MAK v UK* (Application no. 45901/05;

(b) In *Digital Rights Ireland* (5.62-5.78 below), the CJEU was of the view that the EU Data Retention Directive, which the UK Government had strongly promoted, entailed "*a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU"*.[43]

(c) In a recent case about the retention of electronic data, Lord Sumption correctly noted that the ECtHR "*has in the past taken exception to the characterisation of interferences by English courts with private life as being minor*", before once again so characterising the retention of electronic data by the police on an individual associated with a political protest group.[44]

It is hard to think of any other area of human rights law that is characterised by such marked and consistent differences of opinion between the European courts and the British judges who in most respects rank among their most loyal and conscientious followers. To the extent that the law permits, it seems to me that there would be wisdom in acknowledging and seeking to accommodate such differences, which owe something at least to varying perceptions of police and security forces and to the different (but equally legitimate) conclusions that are drawn from 20th century history in different parts of Europe.

Modern attitudes to privacy

2.25. Attitudes to privacy, surveillance, and investigatory powers are frequently surveyed.[45] But the treatment of those surveys requires some care, as results may well be influenced by a wide range of factors, including recent newsworthy events,[46] the exact wording of the question or indeed the identity of the questioner.

2.26. Even within the UK, people vary widely in their attitude to privacy. Research by DEMOS into data sharing places people into different categories, described as: nonsharers (30% of the population), sceptics (22% of the population), pragmatists (20% of the population), value hunters (19% of the population) and enthusiastic sharers (8% of the population).[47] These groups have very different views on issues relating to privacy. Moreover, research has showed that people's own personal

judgment of 23 March 2010)) (duty of care to parents of children suspected to be subjects of abuse) was 1-4 then 7-0.

43 *Digital Rights* Ireland, judgment at para 65.

44 *R (Catt) v Commissioner of Police of the Metropolis and others* [2015] UKSC 9, para 26.

45 Some of those I have considered are: Special Eurobarometer 359, *Attitudes on Data Protection and Electronic Identity in the European Union*, (2011), ("Eurobarometer"); Demos, *The Data Dialogue,* (2012), ("Demos"); Wellcome Trust, "Summary Report of Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data", (2013) ("Wellcome Trust"); Pew Research Center, "Public Perceptions of Privacy and Security in the Post-Snowden Era", (2014) ("Pew, *Public Perceptions"*); Ipsos MORI, "Public Attitudes to Science"*,* (2014), ("Ipsos MORI, *PAS"*); TNS-BMRB Polling 23-27 January 2014, ("TNS-BMRB"); Dr J. F. Rogers, "Public opinion and the Intelligence Services"; (2014) ("YouGov"); Ipsos MORI for ESRC/ONS, "Dialogue on Data: Exploring the public's views on using administrative data for research purposes", (2014) ("Ipsos MORI: ESRC/ONS"); Deloitte, *Data Nation 2014: Putting Customers First,* (2014) ("Deloitte"); Ipsos MORI, "Public attitudes to the use and sharing of their data", for the Royal Statistical Society, (2014) ("Ipsos MORI: RSS"); and Pew Research Center, "Americans' privacy strategies post-Snowden" (2015), ("Pew, *Privacy strategies*").

46 It was stated in Ipsos MORI, *PAS* that the survey may have been influenced by recent NSA leaks and a trial on phone hacking in the UK.

47 Demos.

environment, history and development has a significant effect on their desire or otherwise for privacy,[48] and that attitudes to privacy are highly contextual.[49]

2.27. In relation to privacy as against the state or public authorities:

(a) Public opinion tends to be more supportive of the use of data where there are tangible public benefits.[50] A TNS BMRB poll in 2014 showed that:

- most people (71%) "*prioritise reducing the threat posed by terrorists and serious criminals even if this erodes peoples' right to privacy"*;
- 66% think that British security and intelligence agencies should be allowed to access and store the internet communications of criminals or terrorists;
- 64% back them in carrying out this activity by monitoring the communications of the public at large; and that
- whereas 60% were very or fairly concerned about social media websites such as Facebook monitoring and collecting information about their online activity, and 55% had the same concerns about search engines such as Google, only 46% and 43% had the same concerns about the US and UK Governments respectively.[51]

Further research shows that people see one of the benefits of surveillance as enabling the government to protect them against crime, including terrorism.[52]

(b) Research by YouGov in 2013 showed that 49% of respondents agreed that the UK Intelligence Services should be allowed in some circumstances to hack into calls/emails/text messages of foreign citizens "*with no questions asked*", as against 27% who thought they should not. The equivalent figures for UK citizens were 43% and 33%.[53] Qualitative surveys have however shown concern about being watched by "*Big Brother*".[54]

(c) Whilst surveys show that the government is trusted more than commercial companies,[55] survey participants have expressed concern regarding the

48 See Nancy Marshall, "Privacy and Environment"*,* (1972) Human Ecology, Vol 1 No. 2, 92.

49 See Pew, *Public Perceptions*; Demos, which showed a greater concern regarding "*personal information*" than "*behavioural data*"; Eurobarometer, which showed particular concern for financial, medical and national identity number information compared to photos, social networks, websites and tastes and personal opinions; and Wellcome Trust, which highlighted a number of distinguishing factors, including the degree of risk if it is misused/stolen, the level of security attached to the data, whether it was anonymous or personally identifiable data, the value of the data, whether it was extracted by free choice or compulsion and whether the collector is governmental or private.

50 TNS-BMRB.

51 TNS-BMRB.

52 Wellcome Trust.

53 YouGov.

54 See the Wellcome Trust.

55 See 2.27(a) above, last bullet point, and Ipsos MORI: ESRC/ONS; Deloitte; Eurobarometer. Within the US government at least, there may also be some differentiation; see Executive Office of the President,

government's use of data,[56] particularly in terms of profiling or leaks.[57] Aligned with the concepts of privacy outlined above, the public are particularly concerned about their data being leaked, lost, shared or sold without their consent.[58]

(d) Safeguards appear to be relevant to public levels of trust: where no mention of safeguards is made the balance of opinion is against data sharing within government, but with safeguards half are in favour of such sharing.[59]

2.28. Public surveys have shown particularly low levels of trust in relation to phone companies and ISPs in dealing with data.[60] A recent survey showed only between 4% and 7% had high levels of trust in such companies to use their data appropriately.[61] They also show a general lack of confidence in the security of everyday channels, social media being viewed as the least secure and a landline as the most secure.[62]

2.29. Some studies show differences in approach by age, although these are not consistent. Several surveys show that younger people care less, trust organisations more, and are happier with data collection and use or online surveillance than older generations.[63] However, the TNS BMRB poll showed that younger people gave a higher priority to privacy when weighed against security,[64] and polls in America have shown that most teenagers take steps to protect their privacy online.[65] Again, while far from conclusive, there is some indication that social class may make a difference: lower social classes showed greater levels of discomfort in relation to sharing their data in the Wellcome Trust survey.

The Snowden effect

2.30. The Snowden Documents detailed the alleged extent of surveillance by British and US security and intelligence agencies. Summarised at 7.6-7.7 below and in Annex 7 to this Report, these materials have influenced some people's views on the balance between privacy and security.

2.31. Particularly striking in this regard was the realisation of the extent to which communications were being intercepted in bulk. It was not shocking to discover that no means of communication is immune: that has been the case for as long as mails have been opened and spies secreted behind the arras. But because such techniques were haphazard, risky and resource-intensive, they have generally been used sparingly, and on a targeted basis. Bulk collection of electronic messages, as

Big Data: Seizing Opportunities, Preserving Values, May 2014, in which law enforcement and intelligence agencies were ranked low in terms of public trust.

56 See Ipsos MORI: ESRC/ONS, Deloitte, and Eurobarometer.

57 See Ipsos MORI: ESRC/ONS, and Deloitte.

58 Ipsos MORI, *PAS*; Deloitte; Demos; although it is expected and supported by the public that governmental administrative data is linked and shared between departments; See Ipsos MORI: ESRC/ONS.

59 Ipsos MORI: RSS.

60 Eurobarometer; Ipsos MORI: RSS.

61 Ipsos MORI: RSS.

62 Pew, *Public Perceptions.*

63 Wellcome Trust; Eurobarometer; Pew, *Public Perceptions*; Deloitte.

64 Wellcome Trust.

65 Pew Research Center, "Teens and Mobile Apps Privacy", (2013).

the Snowden Documents brought home, can be achieved with far less effort and so brings the potential (if not properly regulated) for spying on a truly industrial scale.

2.32. Two US surveys by the Pew Research Center highlight the influence of the leaks:

(a) In the 2014 study, most adults did not agree that it was a good thing for government to "*keep an eye*" on internet activity, and adults who had heard about government surveillance were more likely to think that internet oversight by government has drawbacks.[66] Overall, 80% of American adults agreed or strongly agreed that Americans should be concerned about the government's monitoring of phone calls and internet communications, with just 18% disagreeing or strongly disagreeing with that notion. According to the authors, the survey confirmed the "*clear trend"* from support for collection of data as part of anti-terrorism efforts to relative disapproval.[67]

(b) In the 2015 study, over a third of those who had heard of surveillance programs had taken at least one step to hide or shield their information from the US Government, with a quarter changing their use "*a great deal*" or "*somewhat*". However (in apparent contrast to the earlier findings), only 52% were "*somewhat*" or "*very*" concerned about US Government surveillance of Americans' data and electronic communications, as against 46% who were "*not very*" or "*not at all*" concerned.[68]

2.33. Further research undertaken worldwide appeared to show that the Snowden Documents have "*damaged one major element of America's global image: its reputation for protecting individual liberties"*.[69] Older Americans were more likely than younger Americans to find it acceptable to spy on citizens of other countries, though Americans in general (perhaps unsurprisingly) were more likely to approve of US government surveillance of foreign nationals than of US citizens. However, people in other nations found NSA surveillance of foreign nationals to be more objectionable than that of Americans.[70] Indeed, 71% of respondents in a worldwide study, including 70% of those in Five Eyes countries,[71] were strongly opposed to the US monitoring their internet use (with 60% wanting tech companies to secure their communications to prevent this).[72]

---

66 Pew, *Public Perceptions*. A majority of adults disagreed with the statement "*it is a good thing for society if people believe that someone is keeping an eye on the things that they do online*", including 20% who strongly disagreed. 36% agreed with the statement, including 7% who strongly agreed. Just 23% of adults who have heard "*a lot*" about the revelations in the Snowden Documents thought online surveillance was good for society, compared with 46% of those who had heard less about the revelations.

67 Pew, *Public Perceptions.*

68 Pew, *Privacy Strategies*.

69 Pew Research Center, "Global Opposition to US Surveillance and Drones", (2014) ("Pew, *Global Opposition"*). This reflected changes in attitude of both Americans themselves and the global public.

70 Pew, *Global Opposition*.

71 The US, UK, Canada, Australia and New Zealand: see further 8.40-8.41 below.

72 Amnesty International, "Global opposition to USA big brother mass surveillance", (2015) ("Amnesty").

2.34. Such a change in attitudes is less apparent in the UK:

(a) Studies have ranked the UK as one of the countries least concerned by government "*spying*" on internet and mobile communications. Along with France, the UK had the lowest proportion of citizens who were opposed to it (44%) in a global study in 2015.[73]

(b) Indeed, a number of studies showed that most people had already assumed that the type of action alleged in the Snowden Documents was undertaken, and only 27% were of the view that it was too intrusive.[74]

(c) Some recent studies have shown support for the use of data to predict and prevent crimes,[75] though others have shown low levels of trust in the UK Government to use their data appropriately.[76]

2.35. One impact of the leaks in the Snowden Documents in the UK is that they damaged people's belief in the safety of their data; with most believing that neither government nor private companies can now keep their data completely secure.[77] But this has not translated into support for the leaks: in a recent study, only 38% of those polled believed that "*leaks by Julian Assange and Edward Snowden*" were justified.[78]

Is privacy dead?

2.36. Mark Zuckerberg, the founder of Facebook, stated in 2010 that privacy is no longer a social norm.[79] Others have gone further still, declaring it to be dead.[80] In the words of a recent newspaper article:

> "We have come to the end of privacy; our private lives, as our grandparents would have recognised them, have been winnowed away to the realm of the shameful and the secret. ... Insidiously, through small concessions that mounted up over time, we have signed away rights and privileges that other generations fought for, undermining the very cornerstones of our personalities in the process. While outposts of civilisation fight pyrrhic battles, unplugging themselves from the web – "*going dark*" – the rest of us have come to accept that the majority of our social, financial and even sexual interactions take place over the internet and that someone, somewhere, whether state, press or corporation, is watching."[81]

---

73 Amnesty.
74 See TNS-BMRB.
75 Ipsos MORI, *PAS.*
76 Ipsos MORI: RSS; 13% had high trust in the British Government compared to 46% with low trust.
77 Ipsos MORI: ESRC/ONS.
78 TNS-BMRB. Interestingly, there was a gender bias highlighted by this study, with more men than women saying that the revelations would do more harm than good.
79 "Privacy no longer a social norm, says Facebook founder", The Guardian, 11 Jan 2011.
80 E.g. J. Morgan, "Privacy is completely and utterly dead, and we killed it", Forbes.com, 19 August 2014.
81 A. Preston, "The death of privacy", The Observer 3 August 2014.

But such colourful defeatism seems largely confined to the commentariat: [82] no one I have heard from suggested that we have come to the end of privacy, or that routine "*watching*" of our communications by the state happens or should be accepted.

2.37. Reports of privacy's death have therefore been exaggerated. But it may legitimately be asked whether the way we live online has changed our attitudes to privacy and whether, if so, there are implications in this for the proper scope of state investigatory powers.

2.38. It is hard to resist the proposition that notions of privacy have changed in recent years. Many of us display an unprecedented willingness to share once-private information with online contacts, service providers and the general public. For example:

(a) We use free email services, despite many of us being aware or suspecting that the provider makes a profit from using the content of our communications to direct advertising towards us.

(b) We allow our phones to act as mobile tracking devices, as reliable as any professional surveillance team, again with increasing awareness that this information too is liable to be monetised and that it can if necessary be obtained by the state.

(c) Many of us post intimate observations on Twitter and photographs on apps such as Instagram, to a potentially infinite number of recipients worldwide.

(d) We accept (generally without reading them) terms and conditions which allow our data to be used, at the discretion of the service provider, for a bewildering variety of purposes.

(e) We are becoming increasingly aware of the ease with which we can be identified or profiled by anyone who chooses to combine different datasets.

(f) By clicking "*Accept*", we may even enable our data to be sold to (via a data broker) or shared with the governments of the UK or of other countries.

In the words of the well-known cryptographer and writer Bruce Schneier, "*The bargain you make, again and again, with various companies is surveillance in exchange for free service.*"[83]

2.39. But all this does not mean that privacy can no longer be protected, or that attempts to regulate state power should simply be abandoned. Four observations may be appropriate here.

2.40. First, the disastrous consequences that can follow from the over-sharing of private information on social media are becoming more widely known, whether in the form of cyber fraud, sexual grooming, so-called "*slut-shaming*" or online bullying. It should

82 Which is itself polarised: see Pew Research Center, "Digital Life in 2025: the Future of Privacy", (2014), which sets out the broad views of privacy experts.

83 B. Schneier, *Data and Goliath*, 2015, chapter 1. See, generally, 8.65-8.104 below.

not be assumed that privacy norms which have moved so rapidly in recent years are now immutable, or that the direction of travel will not reverse. Indeed, Facebook itself in December 2014 sent an update to users promoting its new "*Privacy Basics*" service, noting that "*protecting people's information and providing meaningful privacy controls are at the core of everything we do"*.[84]

2.41. Secondly, it is clear that most people do care about their privacy, however defined, and take steps to preserve it online.[85] If those steps are ineffective, consumer protection law should be doing more to ensure that only informed consent to the sharing of their data will suffice.[86] Moreover, it is false to assume that there is one standard of privacy that attaches to all electronic communications: people treat different types of information as entailing different levels of privacy (2.26 above), and users of various platforms are mindful of the extent and degree to which that information is available to others.[87]

2.42. Thirdly, the trend away from privacy is counterbalanced by the spread of encryption. Companies make a selling point out of assuring their customers that (as in the case of modern iPhones), not even the provider of the phone will be able to decrypt its contents.[88]

2.43. Finally, the distinction between the activities of service providers and those of the state, though sometimes elusive, is nonetheless real. The state has a duty to protect its citizens. Pursuant to that duty, it asserts the right to intercept communications or collect data without consent, and to use that information for the purpose of depriving persons of their liberty. These powers are asserted, furthermore, even in relation to people in respect of whom there is no reasonable suspicion that they have committed any crime.

2.44. Recent changes in privacy norms are not without relevance: they may for example have a bearing on whether there is a reasonable expectation of privacy in a particular type of data at a particular time. They do not however amount to any sort of argument for dispensing with constraints on the government's collection or use of data. Indeed as more of our lives are lived online, and as more and more personal information can be deduced from our electronic footprint, the arguments for strict legal controls on the power of the state become if anything more compelling.

---

84 Facebook update, 20 December 2014.

85 See Big Brother Watch/ComRes, *Global Attitudes to privacy Online*, October 2013 ("BBW/ComRes").

86 See further 8.85-8.88 below. In the BBW/ComRes survey, 65% of consumers believed that national regulators should do more to force Google to comply with regulations on online privacy and data protection.

87 See A. Watts, "A Teenager's View on Social Media"*,* 2 January 2015.

88 See the Privacy section on the Apple website: https://www.apple.com/privacy/government-information-requests/.

3. THREATS

Introduction

3.1. I am specifically directed by DRIPA 2014 s7 to consider "*current and future threats to the United Kingdom*", of the sort which the capabilities under review could be useful in addressing. The UK faces a diverse range of security threats, from a wide array of perpetrators, including terrorism, organised crime, espionage from hostile states and cyber threats. All of these contribute to a multi-faceted national security threat, to which the threat from crime adds a further dimension.

3.2. The calibration of response to threat is far from an exact science, not least because the perceived severity of a threat depends on the fear that it evokes as well as on its potential for harm. Some harm may be neither tangible nor immediate: for example, long-term damage to the UK's economic wellbeing, or a reduction in the UK's ability to act globally and achieve its international objectives. Such impacts are harder to observe and to quantify than violent attacks. They may never come into the public eye or receive widespread publicity. But without some notion of all these threats, it is hard to pronounce on the extent to which intrusive powers are needed.

3.3. I received a great deal of evidence from the Government, law enforcement and the security and intelligence agencies on the threats faced today and likely to be faced in the future. For the purposes of this short summary, I have grouped them under two headings: national security threats and crime and public safety. But before turning to the detail, I make two preliminary points.

The threat in perspective

3.4. No one doubts the gravity of the threats that are faced by the UK and its inhabitants, or the capacity of those threats both to take life and to diminish its quality.[1] But it is generally a mistake (though a surprisingly common one) to describe threat levels as "*unprecedented*". Two points need to be kept in mind:

(a) Events capable of taking life on a massive scale are a feature of every age and every stage of development.[2]

(b) Whilst some of the threats faced at any given time will be realised, others will not.

3.5. The last point was well made by Jonathan Evans (now Lord Evans of Weardale) in a public speech as Director of MI5:

> "Those of us who are paid to think about the future from a security perspective tend to conclude that future threats are getting more complex, unpredictable and alarming. After a long career in [MI5], I have concluded that this is rarely

[1] I am grateful to Ray McClure, uncle to Fusilier Lee Rigby, for his thoughtful submission to the Review.

[2] The Black Death probably killed at least a third of the population of Europe in the years after 1346. As to violence, Steven Pinker of Harvard University has warned against "*historical myopia*", and claimed that "*nostalgia for a peaceable past is the biggest delusion of all*": *The Better Angels of our Nature* (2011), pp. 233, 838.

> in fact the case. The truth is that the future always looks unpredictable and complex because it hasn't happened yet. We don't feel the force of the uncertainties felt by our predecessors. … At least some of the areas of concern that I have highlighted tonight may turn out to be dogs that don't bark. … On the other hand, the dog you haven't seen may turn out to be the one that bites you."[3]

3.6. The moral is not that threats ought to be ignored: on the contrary, any credible threat should be guarded against. The point is, rather, that claims of exceptional or unprecedented threat levels – particularly if relied upon for the purposes of curbing well-established liberties – should be approached with scepticism.

The importance of good order

3.7. It was said in Chapter 2 that privacy is a prerequisite to individual security, self-fulfilment and the maintenance of a thriving democratic society. So indeed it is: but each of those things depends more directly still upon the population feeling safe, secure and confident that the criminal law in all its aspects will be effectively enforced against wrongdoers.

3.8. The point may seem obvious, but by way of illustration:

(a) A person who lives in fear of anti-social behaviour, online harassment, neighbourhood drug gangs or persistent nuisance calls is patently unable to experience individual security or self-fulfilment.

(b) The trust in strangers on which civilised society depends is eroded by a perception that cyber fraud is prevalent, that rogue tradesmen prey on the old with impunity or that paedophiles flourish in the privacy of their homes.

(c) The threat of terrorist atrocities curtails normal activities, heightens suspicion, promotes prejudice and can (as the terrorist may intend) do incalculable damage to community relations.

(d) A perception that the authorities are powerless to act against external threats to the nation, or unable effectively to prosecute certain categories of crime (including low-level crime), can result in hopelessness, a sense of injustice and a feeling that the state has failed to perform its part of the bargain on which consensual government depends.

3.9. For such reasons, the law plainly states that the right to respect for private life and correspondence can be overridden (where it is necessary and proportionate to do so) in the interests of national security, public safety and the prevention of disorder or crime.[4]

---

3 Lord Mayor's Annual Defence and Security Lecture, Mansion House, (June 2012), para 6.

4 See 5.16 below.

National security threats

3.10. National security is nowhere defined in statute. The Government set out in its 2010 National Security Strategy,[5] annually updated, what it assesses to be the 15 main risks. The highest priority risks are in summary:

(a) terrorism, both Islamist and Northern Ireland-related;

(b) cyber attacks by other states and large-scale cyber crime;

(c) a major accident or natural hazard which requires a national response; and

(d) an international military crisis between states.

The 11 other risks prioritised by the Government include the exploitation by terrorists of instability, civil war or insurgency overseas, a significant increase in organised crime affecting the UK, a significant increase in attempts by terrorists, organised criminals and carriers of drugs and firearms to cross the UK border and disruption to the supply of oil, gas or other resources.

3.11. In a written statement introducing his latest annual report on progress with the national security strategy, the Prime Minister highlighted the major risks and threats that materialised in 2014:

> "Islamist extremism, with most lately the emergence of ISIL, is the struggle of our generation; and we are working closely with international partners to tackle this, deploying UK Armed Forces to combat the emergence of this senseless, barbaric organisation. Russia's illegal actions in Ukraine and conflict in the Middle East have created instability and uncertainty. Tensions in East Asia have added to the risks in that region. Sophisticated and targeted cyber attacks continue to cost the UK economy several billion pounds per year; the dangerous and irresponsible leaking of sensitive information by Edward Snowden has had far-reaching consequences. The Ebola virus is wreaking immense damage in West African nations, and posing a potentially devastating threat to others."[6]

3.12. The strategic response to many of those threats involves the use of covert investigatory powers. In relation to some of them (terrorism, cyber attacks, organised crime), the monitoring of electronic communications is a central and growing part of the response.

Terrorism

3.13. The terrorist threat was recently summarised in the annual report on the Government's CONTEST strategy.[7] Reference was made to:

---

5 *A Strong Britain in an Age of Uncertainty: the National Security Strategy*, Cm 7953, (October 2010).

6 Statement HCWS159 of 18 December 2014, introducing the *Annual report on the National Security Strategy and Strategic Defence and Security Review*, (2014).

7 *CONTEST, the United Kingdom's strategy for countering terrorism: Annual Report for 2014*, Cm 9048, (March 2015).

(a) the raising of the UK threat level in August 2014 from "*substantial*" back to "*severe*" (where it had been for most of the period 2006-2011), meaning that an attack is highly likely;

(b) the 600 or so people with extremist connections to have travelled to Syria and Iraq, some of whom have combat experience and terrorist-related training and many of whom have already returned to the UK;

(c) the "*unprecedented quantity of terrorist and extremist propaganda*" that is fuelling terrorism;[8]

(d) the continued threat from al-Qaida core, al-Qaida in the Arabian Peninsula and al-Shabaab;

(e) kidnap for ransom;

(f) the advocating of attacks by lone operators; and

(g) the continuing threat from Northern Ireland-related and far right terrorism.

678 people in Great Britain (i.e. the UK not including Northern Ireland) were charged with, and 432 convicted of, terrorism-related offences between September 2001 and September 2014. The figures for charge and convictions in the year to September 2014 are 77 and 26 respectively.[9]

3.14. A more detailed account of the threat is contained in my own annual report (normally published in July) on the operation of the Terrorism Acts: recent editions have given details of the major terrorism prosecutions since 2000 and of the 30 Britons killed by terrorism overseas between 2005 and 2013. While noting that Islamist terrorism has afflicted a number of European countries, I expressed the view in 2013 that:

> ".. the threat to the United Kingdom – as measured by the number of serious plots since 2001 and over the past three years – is unfortunately more serious than the threat to other parts of Europe. That deaths of UK nationals through terrorism have not been more numerous owes something to luck ... and a great deal to the capabilities of the intelligence agencies and police." [10]

3.15. In its latest evidence to the Review, MI5 has pointed out some of the recent factors which reinforce their concerns about the terrorist threat. Terrorist related arrests are up 35% compared to 2010. The number who have travelled to Syria and undertaken terrorist training since 2012 is already higher than has been seen in other 21st century theatres, such as Pakistan/Afghanistan, East Africa and Yemen. The threat posed on

---

8 In his evidence of 13 January 2015 to Parliament's Home Affairs Select Committee (HC 933), Rob Wainwright, the Director General of Europol, described the aggressive and imaginative use of the internet by terrorists for recruitment and propaganda as an important evolution, necessitating "*a closer, more productive relationship between law enforcement and the technological firms, and also the right legislation in place to allow the security authorities to monitor suspected terrorist activity online*".

9 Home Office, *Operation of police powers under the Terrorism Act 2000 and subsequent legislation*, (March 2015).

10 D. Anderson, *The Terrorism Acts in 2012*, (July 2013), 2.8-2.26, 2.61; *The Terrorism Acts in 2013*, (July 2014), 2.18 and 2.21.

their return comprises not just attack planning but radicalisation of associates, facilitation and fundraising, all of which further exacerbate the threat. The number of UK-linked individuals who are involved in or been exposed to terrorist training and fighting is higher than it has been at any point since the 9/11 attacks in 2001. MI5 regard this aspect of the threat as unprecedented. Some travellers were previously unknown to MI5.[11]

3.16. The volume and accessibility of extremist propaganda has increased. UK-based extremists are able to talk directly to ISIL fighters and their wives in web forums and on social media. The key risk is that this propaganda is able to inspire individuals to undertake attacks without ever travelling to Syria or Iraq. Through these media outputs, ISIL have driven the increase in unsophisticated attack methodology seen in recent months in Australia, France and Canada

3.17. MI5 have successfully disrupted two attack plots by lone actors in the past nine months, both in the late stages of preparation. But MI5 have explained that identifying such individuals is increasingly challenging, exacerbated by the current limitations in their technical capabilities, which I discuss later.

3.18. Finally, Northern Ireland's progress towards a post-conflict society is unfortunately far from complete. A real terrorist threat persists in parts of Northern Ireland, as the following figures demonstrate:

(a) In the year to February 2015 there were three security-related deaths, 71 shooting incidents and 44 bombing incidents, together with 49 casualties from paramilitary-style assaults.

(b) Over the same 12-month period, 230 persons were arrested in Northern Ireland under the Terrorism Acts, and 37 were charged. [12]

(c) Of the 20 dissident republican attacks during 2014, most were unsuccessful. But the Director General of MI5 has said that "*for every one of those attacks we and our colleagues in the police have stopped three or four others coming to fruition*."[13] My own regular visits to Northern Ireland, where I am briefed in detail by police and security services, give me no cause to doubt that assessment.

The threat level to Northern Ireland from Northern Ireland-related terrorism remains at "*severe*".

Espionage

3.19. Espionage did not go away at the end of the Cold War. Hostile states still seek to gather sensitive intelligence on a wide range of subjects – defence, energy, financial, technological, industrial and commercial – often to advance their own state programmes. When they succeed, they disadvantage the UK economically, militarily

11 Evidence from MI5, April 2015.
12 PSNI, *Security Situation Statistics*, 2015.
13 Andrew Parker, address of 8 January 2015 to RUSI, available on www.mi5.gov.uk, paras 28-29.

and politically. They recruit human agents and use cyber and technical operations to target UK interests.

3.20. The scale and extent of hostile foreign state targeting of the UK means that the potential for future damage of UK interests is high and growing. The spread of the digital world is providing states with many more operational opportunities. The human, physical and cyber assets used by hostile states are often coordinated to enable or complement each other. Cyber espionage allows information to be stolen remotely, cheaply and on an industrial scale at relatively little risk to the hostile state's intelligence officers or its agents. Whatever is thought of Edward Snowden's actions, they demonstrate the impact that can be inflicted by a single well-placed individual with wide network access.[14]

Cyber threats

3.21. A range of hostile actors make use of cyber methods, including online criminals, fraudsters, or money launderers; terrorists threatening violent attacks or disruption of public services and websites, and hostile states conducting cyber espionage to steal information covertly. In many respects the proliferation of online technologies and our increasing reliance on the internet in our day to day lives, and to conduct business, has created a rich pool of opportunities for those seeking to harm UK interests, and has lowered the bar to entry to some actors by providing a cheap, convenient, and deniable way of conducting their activities. I was told of repeated attacks by hostile foreign states on UK Government and industry.

Crime and public safety

3.22. Recorded crime has fallen dramatically in recent years: the Crime Survey for England and Wales **[CSEW]** recorded a total of 7 million crimes committed against resident adults in the year to September 2014, as against 19 million in 1995.[15] There have been similar trends across the western world. Such figures do not, however, tell the whole story.

Organised crime

3.23. Organised crime was estimated by the NCA to be worth £24 billion in 2013, and be perpetrated by 5,800 active organised crime groups in the UK comprising around 40,600 individuals. It includes trafficking and dealing in drugs, people, weapons and counterfeit goods; sophisticated theft and robbery; fraud and other forms of financial crime. It also includes organised child sexual exploitation. Much organised crime is conducted online or is cyber-enabled.

3.24. In some ways organised crime is more complex than terrorism. It is characterised by violence or its threat and but also often depends on the assistance of corrupt, negligent or complicit professionals, notably lawyers, accountants and bankers.

---

14 Evidence from MI5, April 2015.

15 Office for National Statistics **[ONS]**, *A stocktake of crime statistics in England and Wales,* January 2015. The ONS describes the CSEW as "*a valuable measure, on a consistent basis, of trends over time*".

Organised crime is international in nature; and through sophisticated use of the internet criminals can commit crime in the UK from anywhere in the world.[16]

Fraud and cyber crime

3.25. Europol commented in late 2014:

> "In general cybercrime is increasing in scale and impact; while there is a lack of reliable figures, trends suggest considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage.
> ...
> Underground forums provide cybercriminals with a nexus for the trade of goods and services and a hub for networking, creating an organised set of criminal relationships from an otherwise disparate population."[17]

3.26. Attention was drawn to the exploitation by criminals of legitimate features of the internet (anonymisation, encryption, virtual currencies), to the increased sophistication of malware and to the increase of e-commerce related fraud in line with the growing number of online payments. Europol suggested that the trend towards cyber crime techniques, even on the part of traditional organised crime groups, "*may reflect how all serious crime will be organised in the future*". The NCA emphasised to me that the internet has increased the geographical range of organised crime, citing a recent example of Anglo-Australian criminal collaboration.

3.27. Europol's reference to a lack of reliable figures is borne out in the UK: fraud and cyber crime are not included in the CSEW headline estimates. As the ONS observed in its January 2015 "*stocktake*":

> **"**Advances in technology and the rise of the internet have provided new opportunities for criminals to commit crime. This has raised questions as to whether the fall in conventional crimes, as described above, has simply been replaced by new types of crime that are not yet well measured by the statistics."

To illustrate the point, the ONS presented an estimate that 5.2% of card owners were victims of card fraud in the year to September 2014, as against 1% who suffered theft from the person and 0.2% who suffered robbery. In a survey of 2000 web users last year by the Get Safe Online organisation, 51% admitted to having been in some way affected by online cyber scams, such as fraud, ID theft, hacking, online abuse or having their computer infected with a virus.[18] Work is said to be ongoing to incorporate measures of fraud and cyber crime into the main CSEW estimates.

16 Evidence from the Home Office, April 2015.
17 Europol, *The Internet Organised Crime Threat Assessment*, (November 2014).
18 Get Safe Online survey, October 2014.

Sexual offences and abuse

3.28. The overall decrease in crime recorded by the CSEW also masks a rapid increase in sexual offences, which rose in the year to September 2014 by 22% (partly, it is thought, because of efforts to reduce under-recording).

3.29. The problem of child sexual abuse is said by the National Society for the Prevention of Cruelty to Children to be much bigger than shown in official statistics, as most such crimes are neither detected nor reported. A major study estimated that almost 1 in 20 11-17 year olds, and 1 in 200 under-11s, had experienced "*contact sexual abuse*" by other children or adults.[19]

3.30. The Child Exploitation and Online Protection Centre **[CEOP]**, an NCA command, has identified key threats including the online proliferation of indecent images of children, online sexual exploitation (or grooming), self-generation of indecent images and transnational child abuse.

3.31. CEOP estimates that there were some 50,000 individuals in the UK engaged during 2012 in downloading and sharing indecent images of children, often using decentralised or peer-to-peer (or P2P) networks. The volume of extreme images has grown exponentially. The dark net, and the live streaming of child abuse, generally from the developing world and in exchange for payment, have been identified as new ways that UK offenders are sexually abusing children.[20]

3.32. Grooming is another crime greatly facilitated by the internet. Predatory paedophiles no longer need to hang around the school gate. Social media, instant messaging and chat are all used, with a significant proportion of reports involving multiple online environments. CEOP comments:

> "The restrained influencing of a child over several months has been largely replaced by rapid escalation to threats, intimidation and coercion ... a symptom of the availability of thousands of potential victims online at any one time."[21]

It can lead both to on-line offending (e.g. deceiving children into sending indecent images of themselves, or engaging in sexual chat or sexual activity over webcam) and to off-line offending such as meetings for sexual purposes. The director of Europol has publicly stated that "*anonymity provided by TOR* [see 4.62(c) below] *is used by people to abuse hundreds of thousands of children throughout Europe with very little fear of detection and prosecution*".[22]

---

19 L. Radford et al, "Child abuse and neglect in the UK today", National Society for the Prevention of Cruelty to Children (2011), Table 1.

20 CEOP, *Threat assessment of child sexual exploitation and abuse,* (June 2013). In J. Bartlett, *The Dark Net*, (2014), at chapter 4 there is a revealing interview with a paedophile who was drawn to increasingly extreme material by the ease and anonymity of online access.

21 *Ibid*.

22 R. Wainwright, "Cybercrime and the challenges for law enforcement", address to LIBE Committee of the European Parliament, (11 November 2014).

Non-police enforcement

3.33. Not all crime is dealt with by the police or the NCA. For example:

(a) Her Majesty's Revenue and Customs **[HMRC]** and the Home Office's Immigration Enforcement branch deal with serious organised crime as well as localised and individual enforcement matters. The cost to the UK from organised attacks on the tax regimes administered by HMRC was estimated at £4.7 billion in 2011-12.[23]

(b) Local authorities and specialist agencies deal with many other crimes and dangers to public safety including the regulation of gambling, benefits fraud, trading standards, gangmasters and environmental protection.[24]

These are all areas that will need to be addressed for the foreseeable future and, so long as these specialised agencies and other authorities are required to be investigatory and enforcement bodies, they will need the powers to undertake their task effectively.

Public safety

3.34. Public safety, especially dealing with missing and vulnerable persons, is a very significant area of police activity. It is also one that places a high demand for communications data to help in the location and identification of such people.

3.35. In Great Britain the police dealt with an average of 838 missing person reports every day in 2012-13.[25] Some 6% of all communications data requests during the survey conducted by the Association of Chief Police Officers **[ACPO]** in 2012 related to investigations into missing or vulnerable people.[26]

Conclusion

3.36. Investigatory powers, often of a rather basic nature, may assist in the detection and investigation of any crime that is prefaced or followed by electronic communication, whether it is a drugs importation arranged by telephone or a stolen item advertised on eBay.

3.37. More complicated, and serious, are the problems posed by internet-enabled crime. Though a historic force for good, the internet has complicated and magnified the threat in a number of ways:

(a) providing a new platform for some crimes (fraud, sexual grooming);

---

23 Submission received from HMRC.

24 For example, Ofcom told me that in the three years to December 2014, among many other regulatory functions, it conducted 2,753 investigations into offences such as unlicensed broadcasting and the placing on the market or putting into service of apparatus liable to cause harmful interference to users of the spectrum.

25 *Missing persons: data and analysis 2012-13*, NCA (November 2014).

26 Submission received from ACPO.

(b) facilitating the spread of others (terrorist propaganda, indecent images);

(c) creating completely new opportunities for criminality and aggression (malware, denial of service attacks); and

(d) allowing almost infinitely various channels for worldwide communication, some of them highly secure, to be used by criminals.

3.38. As the Director of Europol said to Parliament's Home Affairs Select Committee in January 2015:

> "[I]t is quite clear that we have a pressing and, indeed, rising challenge to deal with highly encrypted communications online that are managed through the space of the darknet, which are effectively out of the reach of law enforcement authorities – not in every case, but in an increasing proportion of those cases. It is fair to say that the scope that the police have to monitor communications in the offline world is greater than it is in the online world. Given that a majority of those communications run by these networks are moving online, there is a security gap there. To what extent it should be plugged by the right and balanced legislation is for others to judge but I do think it is one of the most pressing problems that police face across Europe."[27]

3.39. If such threats are to be effectively countered, no-go areas for law enforcement must be kept to a minimum. As Sir Iain Lobban, Director of GCHQ, said of online criminals in his valedictory address:

> "We have to enter that labyrinth to find them."[28]

I examine how that can best be achieved, and the necessary accompanying safeguards, in later parts of this Report.

27 Rob Wainwright, oral evidence of 13 January 2015 (HC 933).
28 Valedictory speech at the Cabinet War Rooms, (Oct 2014).

4. TECHNOLOGY

Introduction

4.1. Any new law – at least if it is to last as long as RIPA has done – must be couched in technology-neutral language. But that fact cannot alter the need for those who debate that law to have at least some understanding of the relevant technology.

4.2. Different participants in the debate rely on the fact and nature of technological change to promote their arguments. Thus:

(a) Privacy advocates point out that as lives take place increasingly online, the potential for electronic surveillance, and its intrusiveness, are growing exponentially.

(b) Law enforcement and intelligence refer to factors such as the fragmentation of providers, concealment of identity and growth of encryption to emphasise the existence of ungoverned spaces, and point to a growing "*capability gap*".

It is plain that the utility and intrusiveness of new and existing investigatory powers can also be evaluated only on the basis of a sound technical understanding.

4.3. This Chapter is compiled entirely from open-source material. Its purpose is to outline, in layman's terms, some of the basic technological concepts and developments that underlie the legislative debate. It lays no claim to technical authority (though it has been reviewed by technical experts). The lightning pace of change means that it is likely to be in some respects out of date almost immediately. Nonetheless, I hope it may be of value to those who must wrestle with the policy issues in this Report.

Changing methods of communication

4.4 Ours is not the first age to make revolutionary claims for new technology. A fictional professor spoke in 1988 of "*the three things which have revolutionised academic life in the last twenty years*" as being "*jet travel, direct-dialling telephones and the Xerox machine*", adding that with those, "*you're plugged into the only university that really matters – the global campus.*"[1] But changing methods of communication since that time, and in particular the growth of the internet, have eclipsed even those developments in their long-term significance.

From landlines to smart phones

4.5. As recently as 1989, letters and landlines were the main methods of communication.[2] By 2014, fewer than three in ten 16-24 year olds used a landline during a week. 16% of UK households do not have one, and the latest UK Communications Infrastructure

1 D. Lodge, *Small World*, 1988, pp. 43-44, cited by S. Pinker, *The better angels of our nature*, 2011, p. 214.

2 Save where otherwise stated, the facts in 4.5-4.10 are taken from Ofcom's *Communications Market Reports* of August 2011 and August 2014, and from its *Infrastructure Report* of December 2014.

Report suggests the increasing use of internet telephony may eventually lead to the landline network (the public switched telephone network) being turned off.[3]

4.6. The mass uptake of digital technology is progressing at extraordinary speed:

(a) In 2014, 82% of UK homes were connected to the internet compared to 25% in 2000, and 93% of adults owned a mobile phone in 2014 compared to 50% in 2000.

(b) In 2014, for the first time, there were estimated to be more mobile subscriptions than people in the world.[4]

(c) Ownership of smart phones is soaring: 61% of adults owned a smart phone in 2014 compared to 27% in 2011. A comparison across the generations is even more striking, with 88% of 16-24 year olds owning a smart phone, compared to 14% of those over 65.

(d) This explosion in the smart phone market is driving the growth in the number of people accessing the internet using their mobile phone: 57% did so in 2014 compared to 28% in 2011.

Proliferating methods of communication

4.7. Phone calls and texts are being joined by other communication platforms such as instant messaging, video calls and communication through social networking sites. Whilst the adult population in general spent 33% of their total daily communications time using email, this reduced to 19% amongst 16-24 year olds, who favour social networking sites over email. Instant messaging apps have overtaken traditional SMS services. In 2012, 19 billion messages were sent per day on instant messaging apps, compared to 17.6 billion text messages.[5] Since 2012 the number of instant messaging apps has grown considerably.

4.8. A further trend is the growing proportion of consumers in the UK using Voice Over Internet Protocol **[VOIP]**: making a phone call over the internet. The number almost tripled between 2009 and 2014, from 12% to 35%. The upsurge in use of VOIP services is linked to the increased ownership of smart phones and tablets, as these devices have integrated VOIP apps.[6] Household take-up of tablets almost doubled between 2013 and 2014, from 22% to 44%.

4.9. Also striking is the increasing pace of adoption of new technologies. Whilst it took 15 years for half the UK population to get a mobile phone, newer technologies, such as social networking sites, reached this figure in four years.

---

3 A landline is still usually needed to connect to broadband in the home to enable the internet telephony to take place.

4 Anonymous industry speaker at Wilton Park, November 2014.

5 "Chat app messaging overtakes SMS texts, Informa says", BBC News Website, 9 April 2013.

6 In 2015, EE will launch WiFi Calling, which will enable calls to be made over the internet without downloading an app. It will use IP multimedia sub-system technology, described at 4.16 below.

4.10. Overall, there are trends towards an increasing variety of communication methods, an increasing number of devices[7] and an increasing pace of adoption of new technologies, with young adults leading the way.

Global nature of the internet

4.11. The trends outlined above have resulted in a vast increase in data volumes. One exabyte of data is 500 billion pages of text: by 2015, 76 exabytes of data will travel across the internet every year.[8] However, the infrastructure of the internet means data are not territorially bound.[9]

4.12. A network is a group of devices which are linked and so able to communicate with one another. The internet is often described as a "*network of networks*",[10] all of which are interconnected. Communications over the internet take place through the adoption of protocols which are standardised worldwide. A single communication is divided into packets (units of data), which are transmitted separately across multiple networks. They may be routed via different countries as the path of travel followed will be a mix of the quickest or cheapest paths; not necessarily the shortest path. The quickest path will depend upon bandwidth capacity and latency (the amount of data which can be sent through an internet connection and the delay). The result of this method of transmission is increased data flows across borders. For example, an email sent between two persons in the UK may be routed via another country if that is the optimum path for the CSPs involved. The route taken will also depend on the location of servers. The servers of major email services like Gmail, Yahoo and Hotmail are based outside the UK.

4.13. It is estimated that somewhere between 10% and 25% of the world's international telephone and internet traffic transits the UK via underwater fibre optic cables and much of the remaining traffic transits cabling in the US.[11] Whilst the cables are not a recent technological development, having been in use since the 1970s, the amount of data that can be carried has steadily risen. Cables carrying data at a rate of 10 gigabits per second were the norm for most of the 1990s. Data rates of 100 gigabits per second have been available since 2010. By 2014 Google had already invested $300million in 60 terabit (60,000 gigabit) per second fibre optic cables. In 2014, it was reported that researchers in the Netherlands and the USA demonstrated data rates of 225 terabits per second.[12]

---

7 In J. Zittrain, *The Future of the Internet and how to stop it*, 2008, the author warns that the move away from "*generative technologies*" such as personal computers towards "*tethered appliances"* such as iPhones would extend surveillance capabilities (p. 113). MI5 expressed to me the contrary view.

8 B. Schneier, *Data and Goliath*, 2015, chapter 1.

9 There are some exceptions. See J. Goldsmith and T. Wu, *Who controls the Internet? Illusions of a Borderless World*, 2006. Recently some countries have shown a desire for data localisation: 4.42 below.

10 P. Denning, "The ARPANET after Twenty Years", American Scientist 77 (Nov-Dec 1989), p. 531.

11 In L. Harding, *The Snowden Files*, 2014 the author suggests the figure is 25%: see p. 157. GCHQ suggested to me that the figure is closer to 10%.

12 S. Anthony, "225Tbps: World's fastest network could carry all of internet's traffic on a single fiber", Extreme Tech Website, 27th October 2014.

Fragmentation of providers

4.14. The infrastructure of the internet has resulted in the fragmentation of providers of both telecommunications services and communications data. This is illustrated by a comparison of the business models behind a landline call and a VOIP call. Thus:

(a) Landline calls are made through a UK CSP to which the owner subscribes, such as BT or Talk Talk. The CSP knows both endpoints of the call and collects billing data.

(b) Most VOIP services are currently provided by OTT providers, such as Skype. These operate over an internet connection which a CSP has provided.

4.15. Many OTT providers are based overseas, with the result that it is more difficult for UK law enforcement and security and intelligence agencies to obtain information from them. The services provided by OTT providers are often free, and limited subscriber data are collected.[13] In addition, communications data relating to a single communication may not be in a single location due to the collaboration of companies.

4.16. The internet protocol multimedia sub-system **[IMS]** is a framework designed to standardise methods of delivering voice or other multimedia services over an internet protocol packet-switched network. It may reduce fragmentation of providers, as it fuses internet and mobile networks and so allows CSPs to support applications such as VOIP and instant messaging. CSPs will be able to compete with OTT providers in the provision of such applications. However, it is likely to lead to greater fragmentation of communications data as new and common identifiers take over from email and phone numbers across multiple devices.

Difficulties in attributing communications

4.17. The infrastructure of the internet can make it difficult to attribute communications to their sender and so offers a "*cloak of anonymity*" for communications.[14]

4.18. An Internet Protocol **[IP]** address **[IP address]** is the identifier for a device on a network. The address may be static or dynamic and is usually written and displayed in the following format: 172.16.254.1 (IPv4 – 32 bits), and 2001:db8:0:1234:0:567:8:1 (IPv6 – 128 bits). IPv6 is the latest version of the Internet Protocol.

(a) *Dynamic Host Configuration Protocol* is used to allocate IP addresses dynamically to devices connected to a network. For example, CSPs assign an IP address to a router and all devices connected to the router use it to form a private IP network. All the connections from the devices on the private network appear to come from the single IP address assigned to the router by using Network Address Translation. CSPs have a pool of IP addresses which are allocated dynamically in sequence, so that a customer's external IP address

---

13 Talk Talk's submission pointed out that business models are constantly changing in the OTT sector. For example, WhatsApp was free but is now starting to charge in certain circumstances. Colin Crowell described OTT providers as being in "*continual evolution"*, JCDCDB, Oral Evidence, p. 235.

14 *@War*, Shane Harris, 2014, p. 20.

will change and different customers will use the same external IP address, but not at the same time.

(b) *Network Address Translation* is a technique used by CSPs to allow a single IP address to be shared by multiple customers simultaneously, sometimes numbered in the thousands.[15] It became necessary due to a shortage of IPv4 addresses, though things will change as IPv6 is increasingly adopted.

DRIPA 2014 mandated the retention of subscriber data for some categories of IP addresses, namely, those which are static and those which are dynamically allocated in sequence. The Counter Terrorism and Security Act 2015 **[CTSA 2015]** seeks to address the difficulty which arises when IP addresses are shared by a number of users simultaneously, by requiring the retention of "*relevant internet data*"[16] in addition to the shared IP address. However those data are not sufficient to resolve IP addresses in all cases (see 9.51 below); and in any event, a CSP can usually only provide details of the person who pays the internet subscription. This is not necessarily the person who was using a device at a particular time.[17]

4.19. One problem created by the variety of devices now commonly used was highlighted by submissions to the Review. Smart phones and tablets are often shared by a number of users, such as family members. Each of these users may be accessing different applications. This pattern of usage differs from the traditional use of a mobile phone by one person. In light of this, one service provider suggested that in the future investigations will need to be much more user-specific. IP matching can only help with this to a certain degree.

4.20. A further problem for the attribution of communications is that an IP address can be changed by the use of a proxy server so that a communication appears to come from somewhere it does not. A proxy server acts as an intermediary between a device and the internet, changing the IP address from that of the actual sender to that of the proxy server. Many use proxy servers for perfectly legitimate reasons, such as to maintain privacy online. However, some use proxy servers in order to carry out cyber attacks so that the origin of the attack remains hidden. Often such attacks involve numerous proxies.

4.21. Virtual Private Networks **[VPN]** act in a similar way to proxy servers by changing the IP address from that of the actual sender to one provided by the VPN. In the past, VPNs were primarily used by companies to allow their employees to access resources on the company's network remotely. Increasingly, VPNs are used by individuals to protect their privacy and security online. Unlike proxy servers, VPNs also provide secure communications through encryption. Multi-hop VPNs offer significantly higher degrees of privacy and anonymity online as they route traffic through two or more VPNs.

---

15 Home Office, "*Counter-Terrorism and Security Bill Factsheet – Part 3 – Internet Protocol (IP) address resolution"*, 2014.

16 The example given in the factsheet of such data is a port number.

17 See for a further example of the problems surrounding IP matching, "Police face new ethical dilemma in increasingly digital world", The Guardian, 12 January 2015.

4.22. Multipath TCP is an example of an emerging technology likely to have implications for IP matching. Most mobile devices can access the internet through both WiFi and a mobile phone data connection, utilising one or the other at one time. Technologies such as Multipath TCP will enable the splitting of traffic between these two methods of access, increasing the number of requests that will have to be made for communications data and making the IP matching process more complex.

4.23. Mobile Edge Computing is also likely to diminish the quantity of data entering the central network. It brings content closer to the user by moving it from the central network to the edge of networks. The benefits are faster delivery and better quality for the user, for example, less buffering. However, this is likely to mean fewer communications entering the core network and so lesser volumes of data available for collection.

4.24. Nomadic wireless technology provides devices with access to an internet connection within a limited area: for example, the localised WiFi Access Points offered by coffee shops in order to encourage custom. Users are transient and access to the internet by a device can only be traced to a timeslot in the specified premises. If the device connects to the internet elsewhere an identifier called a MAC address will recur, however it is possible to change MAC addresses.

4.25. The internet provides opportunities for undetected communications:

(a) Anyone can set up an email address or social networking profile using a pseudonym.[18]

(b) Criminal gangs can use gaming consoles to communicate.[19]

(c) Opportunities for covert communications via the internet include the use of internet cafes and hidden web pages (see 4.67-4.70 below).

(d) Encryption software, discussed in more detail below, can be used to hide the content of communications.

(e) An instant messaging service called Wickr allows users to send encrypted and self-destructing messages.

New sources of data

4.26. Technological change has also resulted in the explosion of open source information. This describes all information that is in the public domain, such as social networking sites, websites, blogs and many specific open source data and service providers.

---

[18] A glimpse into the future of online identities can be found in patents granted to Apple in 2014 for Automatic Avatar Creation technology and Avatar Reflecting User State technology. The former can create a 3D icon resembling the user, while the latter will allow users to communicate via individualised avatar expressions: L. Gonzalez, "Why Apple thinks 3D Avatars Will be the Future of Online Identities", PSFK, 10th April 2014.

[19] JCDCDB Report, p. 381, citing the evidence of Peter Fahy, Chief Constable of Greater Manchester Police.

4.27. The year 2000 has been identified as the year a social networking site (Friends Reunited) first appeared in the UK,[20] with Facebook and Twitter appearing in 2004 and 2006 respectively. By Q4 2014, there were 1.39 billion monthly active Facebook users. The equivalent figure for Twitter was 288 million.[21] Such sites provide the opportunity for an expansion of what is called Open Source Intelligence **[OSINT]**: the use of open source information for intelligence purposes.[22] In the US, an official report into the events leading up to 9/11 recommended the setting up of an Open Source Agency. A similar recommendation was made in an official report into weapons of mass destruction shortly later. The Open Source Center was established by the Director of National Intelligence in 2005.[23] The Center was charged with collecting information available from "*the Internet, databases, press, radio, television, video, geospatial data, photos and commercial imagery.*"[24] A former head of the bin Laden Unit of the Central Intelligence Agency in the United States noted that "*90% of what you need to know"* comes from OSINT.[25] According to a report in 2010, "*in the aftermath of 9/11, intelligence failures - particularly a deficient consideration of OSINT … - have been identified as major reasons for the inability to anticipate and prevent these attacks.*"[26] In October 2014, James Clapper, the Director of National Intelligence, described social media as "*huge for intelligence purposes*".[27]

4.28. As explained to the JCDCDB by Colin Crowell, Head of Global Public Policy at Twitter, law enforcement can simply go to the Twitter website and locate what they are looking for. Even this may no longer necessary: a social media monitoring platform called Geofeedia allows anyone to "*search, monitor and analyse real-time social media content by location, from anywhere in the world with a single click.*"[28] In addition, social data providers, such as GNIP, provide a one-stop shop for social data.

4.29. UK law enforcement and security and intelligence agencies of course use OSINT, though the extent of that use is not publicly known.[29] By way of example, following a review by the Her Majesty's Inspectorate of Constabulary of the August 2011 disorders

---

20 A. Charlesworth, *An Introduction to Social Media Marketing*, 2014, p.43.

21 See: http://www.statista.com, 2015.

22 In 2012, the term "SOCMINT" was coined to cover Social Media Intelligence (see Sir D. Omand, J. Bartlett and C. Miller, "Introducing Social Media Intelligence (SOCMINT)*"*, (2012) Intelligence and National Security, Vol 27, Issue 6. Others regard it as part of OSINT: see "Social Media Intelligence (SOCMINT) – Same Song, New Melody?", Open Source Intelligence Blog, 31 October 2012.

23 *Open Source Intelligence in a Networked World*, Antony Olcott, (2012), pp. 86-87.

24 See the press release by the Office of the Director for National Intelligence: *ODNI Announces Establishment of Open Source Center*, November 8 2005, see: http://fas.org/irp/news/2005/11/odni110805.html.

25 S. B. Glasser, "*Probing Galaxies of Data for Nuggets*", The Washington Post, 25 November 2005.

26 International Relations and Security Network, *OSINT Report 3/2010*, (2010), p.6.

27 In a speech at the Grand Hyatt Hotel in Washington DC, a copy of which can be found at: http://www.dni.gov/index.php/newsroom/speeches-and-interviews/202-speeches-interviews-2014/files/documents/Newsroom/title=%22Go.

28 See Geofeedia's website: http://geofeedia.com/how-it-works.

29 I am aware that Privacy International have made Freedom of Information requests to law enforcement but that these were refused.

in English cities,[30] an "*all-sources hub*" was created to help police to tackle disorder, which includes social media monitoring.[31]

4.30. The use of location data provided by mobile phones is another example of the "*new dimensions of data*"[32] created by technological change. It comes as a surprise to many smart phone owners to see how much detailed information about their movements is routinely recorded and retained on default settings.[33] The impact of this dimension was brought to life by the German politician, Malte Spitz, in 2009, after he obtained his phone data from Deutsche Telekom and permitted a newspaper to combine that location data with information freely available about him online, in order to produce a detailed map of his movements over a six-month period.[34] This new source of data has become more voluminous in a world full of app update notifications: location data are created by every notification. Tweets posted from mobile phones can also reveal location data, as do Public WiFi services. In February 2015 research was published which shows how information about a user's location can be obtained simply by reading aggregate power usage on a phone. Modern mobile platforms allow applications to read this information.[35] Images taken on mobile phones, and some cameras, also embed location data in the image file.

4.31. These new dimensions of data are ever increasing. The iPhone 5S, introduced in 2013, contains Touch ID technology allowing the user's fingerprint to act as a pass code, as do its successors.[36] Samsung Smart TVs have a voice recognition feature which, if activated, sends voice data over the internet to a voice recognition service. A UK bank is carrying out a trial of technology which uses customers' heartbeats to verify their identity for online banking.

4.32. Tags using radio frequency identification allow the objects to which they are attached or in which they are embedded to be located: they may be used by retailers to track inventory and prevent shoplifting, but also to transmit location information after purchase. Cars are increasingly becoming software platforms: "*black box insurance*" allows premiums to be calculated on the basis of driving behaviour as monitored by telematics, and may also allow emergency services to be notified in the event of a crash and guided to the site by Global Positioning System **[GPS]** technology.[37]

4.33. A source of data predicted to enter the mainstream by 2020 is the Internet of Things **[IOT]** or machine to machine communications. These terms are used to describe the idea of having all electronic devices at home and in the workplace connected to the

30 Her Majesty's Inspectorate of Constabulary, *The rules of engagement: A review of the August 2011 Disorders* (2011).

31 See C. Hobbs et al (eds), *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities*, (2014), p 24.

32 As set out in the Submission I received from Dr Paul Bernal, p. 3.

33 To see where you have been and how long you stayed, on an iPhone 5 or 6 click on Settings, Privacy, Location Services, System Services, Frequent Locations.

34 As can be seen at http://www.zeit.de/datenschutz/malte-spitz-data-retention.

35 R. Whitwam, "Battery power alone used to track Android phones", Extreme Tech Website, 23 February 2015.

36 One of three future trends in the application of biometrics identified by witnesses to the House of Commons Science and Technology Committee Inquiry into biometric data was the proliferation of mobile biometrics: *Current and Future Uses of Biometric data and technologies*, 6th Report of 2014-2015, p. 9, published 7 March 2015.

37 "Little black box under the bonnet saved my life", Mail Online, 10 March 2015.

internet and capable of communication without human intervention. As explained by one journalist:

> "In the World of the Internet of Things, your car, your heating system, your refrigerator, your fitness apps, your credit card, your television set, your window shades, your scale, your medications, your heart rate monitor, your electric toothbrush and your washing machine to say nothing of your phone - generate a continuous stream of data that resides largely out of reach of the individual."[38]

A speaker at a Wilton Park seminar in November 2014 summarised the position as being that in 1975 there were 1 billion connected places; in 2010 there were 5 billion connected people; and that in 2020 there will be 50 billion connected devices. This expansion will be enabled by the latest version of the Internet Protocol, IPv6, which provides a far greater number of IP addresses than existed under IPv4.

4.34. One already common use of IOT is in energy efficiency. An internet-enabled smart thermostat adapts to its user's behaviour patterns by recording energy usage, home temperature, humidity, ambient light and nearby movement.[39] Machine-to-machine communications will make it increasingly difficult to know who owns particular data. Smart meters also provide the potential for malicious disruption: this is the consumer end of the more widespread scope for supervisory control and data acquisition attacks on control systems. It has been suggested that adopting IOT without adequate security will afford major opportunities for surveillance: in the words of Phil Zimmerman, "*You pay good money ... to turn your home into North Korea.*"[40]

4.35. The fastest growing category of IOT is wearable devices. Widely known examples have included Fitbit and Google Glass, but these are just the tip of the iceberg of an industry entering fields such as law enforcement and health. The wearing of body cameras by police is currently being trialled across the UK and 2015 has been predicted to be the year of wearable technology.[41] Indeed, "*Implantables, embeddables and even ingestables are already emerging as the next wave of wearable technology*."[42] This is in line with one of the predictions made by technology experts as to what the digital world will look like in 2025, namely, "*augmented reality enhancements to the real world input via portable, wearable and implantable devices*".[43] The scope for communication by new generations of medical devices (pacemakers, hearing aids, etc.) is clear.

4.36. IOT will lead to the growth in the volume of data, as data are generated on a continuous basis from sensors in these connected devices. In this way, IOT will provide further

---

38 S. Halpern, "The Creepy New Wave of the Internet", The New York Review of Books, 20 November 2014.

39 B. Schneier, *Data and Goliath*, 2015, chapter 1. The manufacturer, Nest, was bought by Google in 2014.

40 CPDP conference, "*Crypto wars reloaded*", Brussels 21-23 January 2015, https://www.youtube.com/watch?v=CcVj5LNwDa8 at 67 min.

41 "2015 gears up to be the year of wearable tech", The Guardian, 25 December 2014.

42 A. Thierer, "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation", (2015) 21 Rich. J.L. & Tech. 6.

43 Pew Research Center, *Digital Life in 2025*, (March 2014). Augmented reality technology superimposes a computer-generated image onto the real-world environment.

fuel for large data sets **[Big Data]**.[44] The development of tools to aid visualisation of Big Data is a growth industry too. It is predicted that there will be 28 billion IOT devices by 2020,[45] and the data transmission speeds made possible by the next generation of mobile network (5G) will fuel this growth.

4.37. Furthermore, IOT is expected to increase the use of cloud computing services: indeed it is predicted that in the next five years 90% of IOT data will be hosted via cloud services. Cloud computing is the term used to describe the delivery of computing resources over the internet on demand. Users can access software via the cloud rather than purchase the software. Another aspect of cloud services is the storing and accessing of data. This makes cloud computing an ideal storage system for IOT as it provides the ability to respond quickly to changes in demand and supply. Since the beginning of 2015, two telecommunications companies have launched cloud-based products to handle data generated by IOT.[46]

Machine learning technologies

4.38. Growth in computer processing capacity and data sets has led to advances in a branch of artificial intelligence called Deep Learning.[47] Deep Learning software mimics the structure of the human brain in order to train computers to see patterns. Research published at the end of 2014 described how image-recognition software is now capable of recognizing and describing scenes, rather than just identifying objects in scenes. The software was developed by training computers to see patterns in pictures and their description using neural networks.[48]

4.39. The Biometrics Commissioner has highlighted the fact that there have been substantial developments in both automated facial and speaker recognition systems in the last few years.[49] The technique involved in Deep Learning is at the heart of some of these recent developments in biometric systems. It has been applied in the area of facial recognition to develop software called Deep Dense, which is able to determine whether an image contains a face, even if part of the face is hidden or upside down.[50] Open Rights Group's submission to the Review highlighted that machine learning technology has been used to teach computers to classify faces based on attributes such as facial expression or hair style. It is also behind advances in speaker recognition systems. The NSA Technology Transfer programme 2013/2014 lists an invention capable of real-time simultaneous identification of multiple voices. One of three future trends in

---

44 See 8.65 onwards for the use of Big Data by private companies. Examples of how Big Data can be used for the common good can be found at http://www.nesta.org.uk/publications/data-good.

45 This was the figure quoted by IBM from analyst firm IDC in announcing cloud services for IOT devices: see http://www.theinquirer.net/inquirer/news/2376409/ibm-announces-internet-of-things- cloud-services.

46 Blackberry announced this on its website: http://press.blackberry.com/press/2015/blackberry-unveils-cloud-based-internet-of-things-platform-.html, and AT&T's launch was announced in early January 2015: http://www.computerworld.com/article/2864069/att-builds-on-internet-of-things-offerings-with-cloud-based-data-store.html.

47 As set out in some detail in MIT Technology Review, *10 Breakthrough Technologies 2013,* see http://www.technologyreview.com/featuredstory/513696/deep-learning/ IBW Watson uses Deep Learning techniques.

48 See e.g. J. Markoff, "Researchers Announce Advance in Image Recognition Software", NY Times, 17 November 2014.

49 *Biometrics Commissioner: Annual Report 2013-2014*, para 336.

50 ""Deep Dense Face Detector" a breakthrough in face detection", TechWorm website, 20 February 2015.

the application of biometrics identified by witnesses giving evidence to the Science and Technology Committee Inquiry into biometric data was the linking of biometric data with other types of Big Data into order to facilitate profiling.[51]

Data mining

4.40. The collection of vast volumes of data enables the identification of patterns and predictions of future behaviour, a process called predictive analytics, data mining or Big Data.[52] An example of this technique is a predictive policing system called PredPol, which analyses large volumes of crime reports to identify areas with high probabilities for certain types of crime. The system has been used by Kent Police to predict when and where drugs crimes and robberies are likely to take place. PredPol is simply about when and where a crime will take place; other technology is aimed at predicting who will commit them. In 2011, the US Department of Homeland Security tested Future Attribute Screening Technology, which seeks to identify potential criminals by monitoring individuals' vital signs, such as cardiovascular signals and respiratory measurements.

Geographical changes

4.41. One of the Snowden Documents stated that the UK had the *"biggest internet access*" in Five Eyes Alliance (made up of the UK, US, Canada, New Zealand and Australia) and added "*We are in the golden age*". However, the growing trend of US ISPs moving to Malaysia and India was also noted and it was suggested that "*traffic will no longer transit the UK*".[53] This movement from west to east reflects the fact that Western Europe and North America are experiencing digital saturation, whilst countries such as India are predicted to drive future growth of the online market. The United Nations predicts that 2015 will be the year when Chinese-speaking users of the internet outnumber English speakers.

4.42. A further trend is the move towards the passage of laws to enforce the localisation of data. In April 2014, Russia introduced a draft law requiring companies to locate servers handling Russian internet traffic locally. This is due to come into effect on 1 September 2015.[54] Brazil introduced a bill containing data localisation proposals, which was later withdrawn. China and Vietnam have passed data localisation laws.[55] Brazil also announced plans in 2014 to build a fibre optic underwater cable between Europe and Brazil. This was reported to be an attempt to reduce Brazil's reliance on US cables to carry communications to Europe.[56]

4.43. All these trends point towards a decreasing bulk collection capability for the West. The golden age may already be passing. This decreasing capability is exacerbated for the

51 *Current and Future Uses of Biometric data and technologies*, (March 2015).
52 V. Mayer-Schonberger and K. Cukier, "At its core, big data is about predictions", (2013) Big Data, p. 11.
53 See "Mastering the internet: how GCHQ set out to spy on the world wide web", The Guardian, 21 June 2013.
54 See Hogan Lovell's Chronicle of Data Protection Blog, Russia Data Localization Law update and webinar, 24 March 2015.
55 M. Bauer et al, "The Costs of data localisation: Friendly Fire on Economic Recovery", ECIPE, No 3/2014.
56 See "Brazil, Europe plan undersea cable to skirt US spying", Reuters, 24 February 2014.

UK by the growth of cloud computing. By 2016, the bulk of new IT spending will be on cloud computing platforms and applications,[57] and the expansion of Network Function virtualisation will mean that cloud providers will be able to host network infrastructure as virtual machines. Most cloud providers are based outside the UK and store data in data centres outside the UK.

Encryption

4.44. Encryption refers to the process of converting information, such as the contents of a message, into unreadable form, so that only someone with the decryption key can read it. It is a crucial part of the transactions we make every day as banks use it to keep data secure during financial transactions. There are a number of types of encryption; for example:

(a) Encryption in transit provides security during the transmission process.

(b) End-to-end encryption provides security at either end of the communication, so that only the recipient, not the company running the messaging service, can decrypt the message.

4.45. The two basic techniques of encryption are symmetric encryption and asymmetric or public-key encryption. Symmetric encryption involves the use of one secret key to both encrypt and decrypt messages. Asymmetric encryption was developed in the 1970s, in an attempt to counter the risks associated with the use of one key. It involves the use of two linked keys; a public key and a private key. A user who wants to send an encrypted message can get the recipient's public key from a public directory. This key is used to encrypt the message, which is sent to the recipient. The recipient can then decrypt the message with a private key.[58]

4.46. The first widely available public-key encryption software was Pretty Good Privacy **[PGP]**, released in the 1990s as a response to the US government's attempt to control encryption via a proposal by the NSA, known as "*Clipper Chip*".[59] The proposal entailed the insertion of a chip into every new piece of electronic device, which would provide encryption for communications. However, all devices containing a chip would be assigned an extra key which would be given to the government in escrow. If the government provided a warrant permitting access to a particular communication this extra key could be used to decrypt the data. Opposition to the proposal was considerable and a number of encryption packages were released in an attempt to derail it. The proposal was ultimately abandoned: but the issue has recently come to the forefront again as a result of the increasing adoption of encryption software.

4.47. This trend towards encryption pre-dates the Snowden Documents, though it is likely to have been accelerated by them.[60] In the year leading up to the release of the Snowden

---

57 The European Internet Forum, *The Digital World in 2030*, March 2014.

58 The story of the invention of public key cryptography is told by S. Singh, *The Code Book*, 1999, chapters 6 and 7.

59 *Ibid.*, pp. 310-311.

60 The Director-General of MI5 told ISC stated that the Snowden Documents "*accelerated the use of default encryption by internet companies…which was coming anyway*": *Report on the Intelligence relating to the murder of Lee Rigby* **[ISC Rigby Report]**, November 2014, para 440.

Documents, crypto-parties (gatherings where hosts teach guests, who bring their digital devices, how to download and use encrypted email and secure internet browsers) had begun to take place in a number of countries, with the aim of bringing *"crypto to the masses*".[61] In January 2014 the British Government launched a campaign called Cyber Streetwise, urging individuals and businesses to protect themselves online.

4.48. Privacy-enhancing changes introduced by Apple in 2014 include encrypting data by default on iPhone devices, a move also made by Google in respect of Android devices. WhatsApp has followed this lead by providing end-to-end encryption for communications. Apple also provides encryption by default on its latest operating systems for laptop and desktop computers. Encryption has been a setting on Apple and Google devices for some years, but now the onus is on the customer to opt out. The encryption of material on the device is now user-controlled, meaning whilst previously Apple could unlock any device using a key that it controlled, it is now unable to unlock iOS 8 devices.

4.49. The level of concern about this trend amongst security and intelligence agencies is demonstrated by the accusation levelled at US service providers by the head of GCHQ that they are becoming the "*command and control network of terrorists*".[62] This is a reference to the fact that terrorists are making increasing use of encryption technologies in order to hide their communications. In 2014, the Director of the Federal Bureau of Investigation in the United States **[FBI]**, suggested that the "*post-Snowden pendulum has swung too far"*,[63] and on 11th January 2015 UK Prime Minister David Cameron announced that if he is leading the next government, he will introduce legislation in 2016 to eliminate "*safe spaces*" for terrorists to communicate.[64]

4.50. However, there are many strands to the encryption debate. A number of Snowden Documents refer to encryption. For example, according to a Briefing Sheet said to relate to an NSA programme called BULLRUN, "*[i]n recent years there has been an aggressive effort, led by NSA, to make major improvements in defeating network security and privacy among many sources and methods.*" An excerpt said to be found in an NSA 2013 Budget Report describes a project called "*SIGINT Enabling*" **as** one which "*actively engages US and foreign IT industries to covertly influence and/or overtly leverage their commercial products designs*".[65] Amongst other things, the program is designed to "*insert vulnerabilities into commercial encryption systems*" and "*influence policies, standards and specifications for commercial public key technologies*". It further states that "*design changes make the systems in question exploitable through Sigint collection … with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact"*.[66] The BULLRUN Briefing Sheet states that "*virtually all decryption is done by PTD*

61 See http://www.cryptoparty.in/.
62 "GCHQ chief accuses US tech giants of becoming terrorists' networks of choice", The Guardian, 3 November 2014.
63 "FBI Chief Comey Hints at Phone Encryption Regulations Suggesting the Pendulum of Privacy has 'Swung too Far'", iDigitalTimes website, 17 October 2014.
64 "David Cameron pledges anti-terror law for internet after Paris attacks", The Guardian, 12 January 2015.
65 The term **[SIGINT]** is used to refer to Signals Intelligence.
66 "Secret Documents Reveal NSA Campaign against Encryption", NY Times, 5 September 2013.

(ARTHUR) processing" - PTD is reported to be a group based at GCHQ.[67] As part of a programme called EDGEHILL, it was said that GCHQ hoped to break the encryption codes of 15 major internet companies and 300 VPNs by 2015.[68]

4.51. The response of Office of the Director of National Intelligence to publication of these documents was that it should not be surprising that security and intelligence agencies seek ways to counteract encryption. Bruce Schneier commented: "*Cryptography forms the basis for online trust. By deliberately undermining online security in a short-sighted effort to eavesdrop the NSA is undermining the very fabric of the internet*".[69]

Back doors and front doors

4.52. The reference to "*design changes*" at 4.50 above appears to denote "*back doors*", which have been defined as access points that enable "*the creator of software or hardware (to) access data without the knowledge or consent of the user*".[70] There may be said to be a back door if anyone other than the communicating parties and service providers has access to a communication.

4.53. The term "*front door*" was described by the Director of the FBI, James Comey, as a door which is "*built transparently*" so that "*the chances of a vulnerability being unseen are much lower*" than with a back door.[71] The Director of the NSA, Mike Rogers, stated during an address on 23 February 2015 that the term back door sounds "*kind of shady*"[72] and suggested the creation of a legal framework whereby access via a "*front door*" would provide access to a communication on possession of a warrant. A door is however a door, and the difference between front and back generally relates to the acknowledgment of its existence rather than to any technical distinction.

4.54. The technology industry tends to be opposed to the idea of any kind of door because the additional code that has to be written in to create the door increases the risk of improper access to the system, and thus consumer confidence in their products.[73] In the words of two encryption experts:

> "[A] 'back door' … increases the 'attack surface' of the system, providing new points of leverage that a nefarious attacker can exploit. It amounts to creating a system with a built-in flaw. … If companies like Apple, Google, Microsoft, and Cisco (just to name a few) are somehow forced to include governmentally mandated flaws in their products, these flawed systems become part of our

67 *Ibid*.

68 "Revealed: how US and UK spy agencies defeat internet privacy and security", The Guardian, 6 September 2013.

69 *Ibid*.

70 S. K. Pell, "Jonesing for a Privacy Mandate, Getting a Doctrine Fix-Doctrine to Follow", (2013) North Carolina Journal of Law and Technology, Vol. 14, Issue 2, ("Jonesing for Privacy") p. 532.

71 In a webcast by the Brookings Institution, "Going Dark: Are Technology, Privacy and Public Safety on a Collision Course", 14 October 2014: https://www.youtube.com/watch?v=Dkbh5fJoFhc.

72 "NSA director defends plan to maintain 'backdoors into technology companies", The Guardian, 23 February 2015.

73 Alex Stamos, Yahoo's Chief Security Officer was reported in the Washington Post as comparing the building of back doors to "*drilling a hole in a windshield*": "Clinton is looking for a middle ground on encryption that experts say doesn't exist", the Washington Post, 25 February 2015.

> national critical infrastructure, and the stakes become a lot higher than hacked cell phone photos or our address books."[74]

The experts to whom we spoke told us that if one government can gain access through a door, so can other governments and private actors. Sooner or later the existence and knowledge of how to exploit such flaws will be discovered via research, serendipity, bribery or coercion. An increasing number of companies – including for example Microsoft, Google and Adobe - offer significant rewards programmes to individual and companies who can identify weaknesses in their software.

4.55. An alternative to back doors is the use by governments of hacking capabilities and malware, often referred to as CNE. The idea is to exploit natural weaknesses in subjects' devices rather than increase security vulnerabilities via back doors.[75] "*Individualised solutions*" was an approach put forward by FBI General Counsel Caproni for that percentage of criminals that use sophisticated technologies.[76] In February 2015, the use of CNE in the UK was acknowledged by the publication of the draft code of practice on interference with equipment **[Draft Equipment Interference Code]**.[77]

Quantum Computing

4.56. Concern about the growing use of encryption has led to the search for ways to counter the technology. The NSA is said to be carrying out research into building a quantum computer,[78] which would be able to break current encryption. Estimates as to when the first quantum computer is likely to appear range from 5-20 years. In November 2014, the Government announced the creation of a national network of Quantum Technology Hubs that will explore the properties of quantum mechanics as part of the UK National Technologies Programme.[79] However, designing quantum-resistant cryptography is a "*difficult task*", according to the Communications- Electronics Security Group based at GCHQ.[80]

Steganography

4.57. In addition to encryption software, software exists which allows messages to be hidden in images, a process called steganography. Camouflage is one such software programme. It hides files by scrambling them and attaching them to a cover file, which acts as a carrier for the secret file. A United Nations Report from 2012 describes how members of the Revolutionary People's Liberation Party Front used Camouflage to hide data within images in JPEG and graphics interchange format files.[81] Professor

---

74 J. Vagle and M. Blaze, "Security "Front Doors" vs "Back Doors": A Distinction Without a Difference", Just Security website, 17 October 2014.

75 Jonesing for Privacy, p. 540.

76 *Ibid.,* p. 542.

77 See further 6.24-6.31 and 7.63-7.65 below.

78 "NSA seeks to build quantum computer that could crack most types of encryption", Washington Post, 2 January 2014.

79 See the press release by the Engineering and Physical Sciences Research Council, on their website at: http://www.epsrc.ac.uk/newsevents/news/quantumtechhubs/ .

80 P. Campbell and others, "Soliloquy: A Cautionary Tale", (2014), available freely on the internet.

81 United Nation Office on Drugs and Crime, *the Use of the Internet for Terrorist Purposes,* (2012), p. 56.

Alan Woodward has warned that moves to ban encryption could result in those who wish to do harm using steganography instead.[82]

Will the encryptors always win?

4.58. The efficacy of legislation aimed at combating encryption has been questioned by some, as there are ways to avoid detection.[83]

4.59. There is force in the argument: but it reckons without human fallibility. Fingerprint databases are a staple of police work, despite the fact that criminals need only wear gloves to render them useless. Similarly, even when encryption cannot easily be broken or circumvented, criminals will not always operate it properly. Thus:

(a) FBI General Counsel Caproni told the US Congress at a hearing about changing technologies in 2011 that the majority of targets "*tend to be somewhat lazy, and a lot of times resort to what is easy*".[84] However, some argue that due to the expansion of encryption, targets are likely to end up using it. The growth of encryption by default settings makes encryption easier.

(b) As Lord Carlile QC explained to the JCDCDB in 2012, criminals still make calls on lines that are listened to and send texts that can be tracked.[85]

(c) The 2014 investigation by the ISC into the murder of Fusilier Lee Rigby revealed that one of those responsible, Michael Adebowale, used his landline to communicate with a member of Al-Qaida in the Arabian Peninsula.

4.60. End-to-end encryption can provide a high level of privacy for the content of communications. However, pattern analysis of communications data can still identify targets. As Charles Farr of the Office for Security and Counter-Terrorism **[OSCT]** explained to the JCDCDB: "*if you have the right kind of data, issues of anonymisation cease to be a significant problem*".[86] The ISC Privacy and Security Report noted that bulk interception was chiefly to GCHQ not for the content of communications so much as for "*the information associated with those communications*".[87]

4.61. Establishing patterns via communications data becomes more difficult when a greater proportion of communications data are encrypted or there are less communications data. The amount of communications data visible to CSPs is decreasing because OTT providers, increasingly use Secure Sockets Layer[88] (SSL) to provide encryption. This means that communications data such as the sender and recipient of an email are not visible to the CSP. When SLL is used the CSP will only see that the message is to be delivered to the particular OTT provider. As mentioned earlier, OTT providers are usually based overseas and so ease of access to this communications data by law

82 "Viewpoint: Criminals can hide data in plain sight", BBC Website, 28 August 2012. He reiterated his warning on 12 January 2015 on Twitter: https://twitter.com/profwoodward.
83 Jimmy Wales, JCDCDB, Oral Evidence, p. 196.
84 Jonesing for Privacy, p. 542.
85 JCDCDB, Oral Evidence, p. 279.
86 *Ibid.* p. 11.
87 ISC Privacy and Security Report, para 80.
88 Websites which use secure sockets layer start with https.

enforcement and security and intelligence agencies via warrant or court order is reduced. In addition, there are an increasing number of anonymity tools which offer to hide communications data. Furthermore, there are some OTT providers which do not store communications data at all (e.g. riseup.net, dukgo.com). The diagrams in Annex 5 to this Report set out the impact of these trends on lawful access to content and communications data.

The dark net

4.62. Three commonly used categories of websites are as follows:

(a) The ***open web*** describes those web pages that are found using standard search engines such as Google.

(b) The ***deep web*** makes up the vast majority (c. 90%) of web pages and describes those sites which cannot be found using standard search engines: intranet pages, administrative databases and personal photo collections.

(c) The ***dark net*** (or dark web) is a tiny part of the deep web, consisting of tens of thousands of websites: the operators of these websites use sophisticated anonymity systems such as The Onion Router **[Tor]** or the Invisible Internet Project to conceal their identities. The dark net has been described as "*a world of complete freedom and anonymity...where users say and do what they like, uncensored, unregulated, and outside of society's norms.*"[89] This enables it to be used by whistleblowers and political activists who rely on anonymity, but also for black market sales and (in common with many non-dark net sites) child pornography.

4.63. Perhaps the best-known dark net site is Silk Road, which used anonymity software to provide a marketplace for illegal goods, such as weapons and drugs. Payment for the goods took place using a digital currency called Bitcoin, which operates outside the banking system and relies on encryption to ensure its integrity. Illegal drugs and other goods to a value of more than $1.2 billion were sold to some 150,000 customers between February 2011 and July 2013, using an eBay-style format in which buyers could grade sellers for their reliability and the quality of their goods.

4.64. Policing the dark net is extremely challenging but not necessarily impossible, as demonstrated by the fact that the first version of Silk Road was taken down by authorities in 2013 and by the success of Operation Onymous in November 2014, an international operation which resulted in the shut-down of dozens of dark net sites including Silk Road 2.0.[90]

89 J. Bartlett, *The Dark Net,* 2014, p.3. For Tor, see 4.67-4.69 below.

90 "Silk Road 2.0 targeted in 'Operation Onymous' dark-web takedown", The Guardian website, 7 November 2014.

Anonymity and anti-surveillance tools

4.65. Users of the open web who take no steps to protect their anonymity reveal information about themselves which can be used to track the online activities of a device and to ascertain the identities of its users. For example:

(a) The content of communications (e.g. emails) may be monitored by anyone with access to the relevant network infrastructure, though this may be technically challenging as well as unlawful.

(b) The IP address which every device must have in order to request and receive content from websites can be recorded by the website operator.[91]

(c) Cookies (text files placed by certain websites on the devices of their users) may enable e.g. a search engine operator to remember a user's recent search terms. That information may be passed on to third parties who can use it for targeted advertising.

4.66. Simple ways of hiding one's identity include the deletion of web browsing histories and the use of pseudonyms on social media sites. More sophisticated anonymity systems offer stronger protection. According to a recent research note from the Parliamentary Office of Science and Technology:

> "Technologies that anonymise internet users have become increasingly popular in recent years. They help citizens to protect their security and privacy and to circumvent censorship. They also facilitate organised crime, such as the billion dollar drug market known as Silk Road."[92]

Those technologies can be divided into centralised trust systems such as VPNs, in which a single entity (usually the provider of the service) can know the identity of all users and their communications partners, and distributed trust systems, in which this is not the case.

4.67. The best-known distributed trust system is Tor (4.62(c) above), which consists of:

(a) The Tor Network: some 6000 computers, provided by volunteers and forming a global network of nodes; and

(b) free software that enables the computers of some 2.5 million Tor users to access the Tor Network, encrypting a user's data and relaying them through several nodes so as to hide the user's IP address and other identifiers.

4.68. The Tor Project claims that c.98.5% of traffic on the Tor Network is from users accessing the open web. It may thus be a valuable tool for anonymous activism, dissident activity, victims of digital abuse such as cyber stalking and even covert online surveillance by law enforcement authorities. Tor provides special nodes called bridges

91 IP addresses may be linked to an individual device, but are sometimes shared or re-allocated as users connect and disconnect from the internet. IP resolution, facilitated by the CTSA 2015, aids the process of linking device to IP address. See 4.18 above.

92 "The dark net and online anonymity", (March 2015). That note is extensively relied upon in this section.

to help users living in regimes such as China, which explicitly block the Tor network. It was reported in 2014 that Russia had offered a reward of 3.9 million roubles to anyone able to develop a way to identify Tor users. The Tor Project received funding in 2014 from bodies including the US Departments of State and of Defense.

4.69. More controversial, and potentially sinister, are the Tor Hidden Services **[THS]** websites (some 40,000 in 2013, identified by .onion addresses), accessible only via the Tor network. Research is difficult, but it is clear that some at least of these websites host criminal markets (most famously Silk Road) and indecent images of children. Law enforcement has enjoyed limited success in de-anonymising Tor users and shutting down THS sites. The Snowden Documents allege that, as of 2012 at least, Tor was considered a "*major"* problem for security and intelligence agencies.[93] But the Parliamentary Office of Science and Technology references doubts over whether it would be technologically feasible to legislate against the availability of THS in the UK.

4.70. Following the release of the Snowden Documents there is evidence of a growing anti-surveillance market.[94] The latest tool to be released by a coalition of human rights and technology organisations is called DETEKT. This scans computers for traces of surveillance technology called Finfisher and Hacking Team RCS, which has been reported to have been used to target human rights activists and journalists in countries all over the world. A project is also said to be underway to develop an International Mobile Subscriber Identity **[IMSI]** catcher detector.[95]

Decentralised networks

4.71. Concern regarding government surveillance has led to a growth in the number of initiatives aimed at decentralising the internet. The purpose of a project called Ethereum is to "*decentralise the web*"[96]: it seeks to do this by using the technology behind the Bitcoin currency and applying it to a variety of services. Maidsafe provides a decentralised internet platform by using the spare space on users' hard drives to store data rather than the servers of large tech companies.[97] In addition to these initiatives to decentralise the internet, a number of applications have emerged which use mesh networking technology to communicate rather than the internet. Vodafone referred to the fact that during recent protests in Hong Kong, protesters used a mesh networking application called Firechat to communicate. By doing so users could bypass Chinese government censorship and potential disablement of cellular networks.

93 "Prying Eyes: Inside the NSA's War on Internet Security", Spiegel Online, 28 December 2014.
94 Following the release of the Snowden Documents it was widely reported that the Indian High Commission in London had reverted to old technology, namely, the typewriter.
95 See 4.72-4.74 below.
96 https://www.ethereum.org/.
97 http://maidsafe.net/.

New capabilities

IMSI catchers

4.72. Interception capabilities in relation to mobile phones are considerable, due to the increasing sophistication of devices called IMSI catchers or IMSI grabbers.[98] These devices intercept signals between a mobile phone and a mobile phone base station, by mimicking the mobile phone base station.

4.73. The capabilities of the devices vary considerably. Some collect IMSI and International Mobile Station Equipment Identity numbers of mobile phones within the range of the device. These unique identifying data can then be used to identify the owner of the mobile phone. More sophisticated devices have the ability to intercept outgoing calls and text messages. Some can even alter the content of a text message and block calls. The most sophisticated devices can deploy malware.

4.74. Reports suggest that the devices have been attached to aeroplanes,allowing collection over a wide area. They are sold on the open market for as little as £100, and body-worn versions are available.[99]

4.75. Rather more simply, man-in-the-middle attacks using WiFi are now commonplace. Access Point names may be duped, and both data and metadata collected easily. Demonstrations of such systems in use are often given at security events to reveal how vulnerable most people are around WiFi and mobile devices.[100] Software and techniques for extracting WiFi passwords is also widely available.

Geotime

4.76. It was reported in 2011 that Geotime software had been purchased by the Metropolitan police. This is said to aggregate information gathered from social networking sites, GPS devices like mobile phones, financial transactions and IP network logs to build a detailed picture of an individual's movements.

Location data

4.77. Advances in technology have not only increased the opportunities for SIGINT. Surveillance methods have also become more sophisticated. For example, it has been seen that location data can be tracked by intercepting mobile phone towers. However, the advent of Google Maps means such information can also be obtained by intercepting Google Map queries on phones. According to a leaked GCHQ

---

98 Brand names for these devices include DRTboxes and Stingrays. The existence of safeguards against the misuse of these devices by police and other public authorities was the subject of a written question in the House of Lords at the end of 2014. The response given was that investigative activity involving interference with property or wireless telegraphy is regulated by the Police Act 1997 and the Intelligence Services Act 1994 **[ISA 1994]**: Hansard HL 11 November 2014 Written Answers col 24.

99 See S.K. Pell and C. Soghoian, "Your Secret Stingray's no Secret Anymore: The Vanishing Government over Cell Phone Surveillance and its impact on National Security and Consumer Privacy", (2014) Harvard Journal of Law and Technology, Vol 28, No 1.

100 How to hack Wifi | Evil Twin Access Point | Man in the Middle Attack | MITM | (https://www.youtube.com/watch?v=aIyKZuxNRnk).

document from 2008, "*anyone using Google Maps on a smart phone is working in support of a GCHQ system*".[101]

4.78. Software and apps that openly reveal location history and track mobile phones, such as Google Location History, GPS Tracking, or Life 360, can be used e.g. by parents to track their children but may also be useful to the authorities. These may use the in-built GPS functions of mobile phones, as well as the geolocation enabled by the cellular network.

Deep packet inspection

4.79. Real-time surveillance has been made possible by deep packet inspection technology **[DPI]**.[102] Before DPI, the internet was akin to a "*daydreaming postal worker*",[103] moving packets around without caring about the content. DPI technology allows the examination of all the different "*layers*" of a communication, including the content layers. It has valuable functionality for legitimate users such as in Security Operations Centres and malware detection and prevention, but also can be used for invasion of privacy.

101 "Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data", The Guardian, 28 January 2014.

102 DPI technology provides an example of technology developed for certain purposes having a ripple effect. One of the primary purposes for which DPI technology was developed was to counter security threats by allowing an ISP to examine all 'layers' of a communication. In C. Fuchs, "Implications of Deep Packet Inspection Internet Surveillance for Society", (2012) Privacy & Security Research Paper Series, #1, the author describes what he calls "*surveillance creep*", namely, "*DPI usage for one purpose...may creep to other more privacy-sensitive activities*".

103 L. Lassig, *Code and other Laws of Cyberspace*, 1999.

PART II: CURRENT POSITION

Part II of the Report (CURRENT POSITION) explains the international legal backdrop, the current powers and the way in which they are used.

- **Chapter 5 (LEGAL CONSTRAINTS)** sets out the legal framework which governs action in this field. In the absence of a written constitution, the chief limitations on freedom to legislate are those imposed by the ECHR and (within its field of application) EU law.

- **Chapter 6 (POWERS AND SAFEGUARDS)** summarises the existing UK laws under which public authorities may collect and analyse people's communications, or records of their communications. It introduces the key concepts and summarises the various powers both under RIPA and outside it, together with the principal oversight mechanisms.

- **Chapter 7 (PRACTICE)** explains how those powers are applied in practice by intelligence, police, law enforcement and others, touching also on data-sharing, bulk personal datasets and the recently-avowed power of computer network exploitation.

- **Chapter 8 (COMPARISONS)** provides three sets of benchmarks which may assist in working out how UK law on investigatory powers should look. These are:

    - ***other forms of surveillance*** (directed and intrusive surveillance, property interference, CHIS &c.),

    - the ***laws of other countries***, particularly in Europe and the English-speaking world, and

    - the use made of individuals' communications by service providers, retailers and other ***private companies***.

5. LEGAL CONSTRAINTS

5.1. This Chapter explains the legal constraints governing UK legislation. The UK is unusual in lacking a written constitution with which all legislation must conform. It has however accepted a number of limitations on its freedom to legislate, including (so far as is relevant here) protections for persons within its jurisdiction against undue interference with their fundamental rights.

5.2. The principal constraints on Parliament's freedom to legislate in relation to investigatory powers derive from European treaties:

(a) The ***ECHR***, a treaty not of the European Union **[EU]** but of the Council of Europe. The ECHR confers rights on individuals within the jurisdiction of its 47 contracting states, enforceable by individual petition before the ECtHR in Strasbourg. Most of the same rights are given effect before the courts of the UK by the HRA 1998, where they must generally be pleaded before any application is made to Strasbourg. Neither the UK courts nor the ECtHR has the power to strike down primary legislation, but each may declare that it infringes ECHR obligations.

(b) The law of the EU, and in particular the ***EU Charter***, which like the underlying general principle of fundamental rights, constrains the law-making powers of the EU and of its Member States when acting within the scope of EU law.[1] National security remains the sole responsibility of each Member State:[2] but subject to that, any UK legislation governing interception or communications data is likely to have to comply with the EU Charter because it would constitute a derogation from the EU directives in the field.[3]

For the sake of completeness, this Chapter also briefly considers the requirements of the common law and of international law, though neither provides any significant additional constraint on Parliament's freedom to legislate in this sphere.

The common law

5.3. The unwritten constitution of the UK is founded on the doctrine of parliamentary sovereignty. The courts may declare the law in areas untouched by statute, and interpret statutes once enacted. They can and do review the actions of the executive (including Ministers and security and intelligence agencies) and hold that they were invalid on various grounds via judicial review. But they have, as a rule, no power to

1 EU Charter, Article 51, as interpreted by the CJEU in Case C-617/10 *Åkerberg Fransson*, judgment of 26 February 2013, para 21 EU:C:2013:105, and (in the context of biometric data retention) Joined Cases C-446 to C-449/12 *Willems*, judgment of 16 April 2015 EU:C:2015:238. I gave written and oral evidence on the scope of the EU Charter to the House of Commons European Scrutiny Committee in the early part of 2014 for its report on the application of the EU Charter in the UK, HC 979, March 2014: https://terrorismlegislationreviewer.independent.gov.uk/eu-charter-of-fundamental-rights/.

2 Treaty on the European Union **[TEU]**, Article 4(2). The scope of that provision (and hence of EU law) has not been definitively resolved (though see Case C-300/11 *ZZ v Secretary of State for the Home Department*, EU:C:2013:363, para 38), and is disputed in current litigation.

3 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data **[Data Protection Directive]** and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector **[e-privacy Directive]**.

set aside or refuse to give effect to duly enacted primary legislation.[4] Judge-declared common law is thus no impediment to the exercise by Parliament of its law-making powers, though clear words are required to override a fundamental right.[5]

5.4. Attempts to fashion a common law constraint on the bulk collection of data have focussed on 18th century cases concerning "*general warrants*". In 1762, the Home Secretary, the Earl of Halifax, issued a general warrant to search for Mr John Entick, who had written libellous publications concerning both the king and his Parliament. The warrant also authorised its executors to "*seize and apprehend, and to bring, together with his books and papers, in safe custody before me to be examined concerning the premises and further dealt with according to law.*"[6]

5.5. The Lord Chief Justice, Lord Camden, held that:[7]

> "... we can safely say that there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society; for papers are often the dearest property a man can have... This is the first instance of an attempt to prove a modern practice of a private office to make and execute warrants to enter a man's house, search for and take away all his books and appears, in the first instance, to be low, which is not found in our books."

5.6. A similar view was taken in the later case of John Wilkes. In 1763 Wilkes wrote a pamphlet critical of George III. Considering that the pamphlet was seditious, a Secretary of State issued a general warrant authorising the police to search for and identify the author, the publisher and their associates.

5.7. Some of those subjected to this treatment challenged the warrant in the courts, which agreed that the Government had acted outside the bounds of its powers. In one case, Lord Chief Justice Pratt stated that:

> "To enter a man's house by virtue of a nameless warrant, in order to procure evidence, is worse than the Spanish Inquisition."[8]

The same judge noted in another case:

> "The defendants claimed a right, under precedents, to force persons' houses, break open escrutores, seize their papers, &c, upon a general warrant, where no inventory is made of the things thus taken away, and where no offenders names are specified in the warrant, and therefore a discretionary power given to messengers to search wherever their suspicions may chance to fall. If such a power is truly invested in the Secretary of State and he can delegate this

4 Save where EU law so requires, as Parliament itself provided in the ECA 1972. Three judges suggested that parliamentary sovereignty might not be absolute in *R (Jackson) v Attorney General* [2005] UKHL 56.

5 *Morgan Grenfell v Special Commissioner of Income Tax* [2002] UKHL 21; [2003] 1 AC 563, para 45.

6 *Entick v Carrington* 95 E.R. 807, p. 810.

7 *Ibid*., pp. 817-18.

8 *Huckle v Money* (1763) 2 Wilson 205 95 ER 768.

power, it certainly may affect the person and property of every man in this kingdom and is totally subversive of the liberty of the subject."[9]

5.8. These are celebrated cases, which have not been overruled. But they have not formed the basis of a common law right of privacy, for two reasons.

5.9. First, they were not explicitly decided by reference to the concept of privacy. The law of trespass applied, so the judgments focus on property rather than privacy issues.[10]

5.10. Secondly, the courts have rejected attempts to rely on those cases as authority for the principle that there is a common law right to private communications.

(a) The High Court held in 1979 that the 18th century warrant cases did not provide a basis for a claim to privacy in respect of phone tapping.[11] Indeed it rejected the idea that there was any common law right to privacy in phone calls. Vice-Chancellor Megarry concluded that it was for Parliament to legislate to protect privacy if it wanted to, and that the right to private communications does not exist in the common law.[12] Mr Malone had therefore to go to the ECtHR in order to establish that he had a right to communicate in private and that the interferences with that right had not been in accordance with the law.[13]

(b) In a recent case before the IPT,[14] the Tribunal was not persuaded that these cases added anything to the analysis.

5.11. The perhaps surprising outcome is that the common law, shorn of the influence of the ECHR, barely recognises the right to privacy or private communications.[15]

The European Convention on Human Rights

Legal framework

5.12. The Council of Europe is an international organisation established in 1949 and currently numbering 47 European states as its members. In 1950 the Parliamentary

9 *Wilkes v Wood* (1763) Lofft 1, 98 ER 489.

10 Though when communications were written on paper, concepts of property and privacy were closely related; and these cases played a part in enabling American judges to derive privacy rights from, in particular, "*the right of the people to be secure in their persons, houses, papers, and effects*" in the 4th amendment to the US Constitution.

11 *Malone v Commissioner of Police* (*No. 2)* [1979] 1 Ch 344, pp. 368-369.

12 *Ibid.*, pp.372-374.

13 *Malone v UK*, (Application no. 8691/79; judgment of 2 August 1984).

14 *Liberty and others v The Secretary of State for Foreign and Commonwealth Affairs and others*, Case Nos. IPT/13/77/CH; 13/92/CH; 13/194/C and 13/204/CH, [2015] UKIPTrib 13_77-H **[Liberty IPT Case]**, judgments of 5 December 2014 and 6 February 2015.

15 See *Kaye v Robertson* [1991] FSR 62, per Glidewell LJ with whom Bingham and Leggatt LJJ agreed: "*It is well known that in English law there is no right to privacy and accordingly no right of action for breach of a person's privacy*"; *Wainwright and another v Home Office*, [2003] UKHL 53; [2004] 2 AC 406, per Lord Bingham, para 26: "*All three judgments are flat against a judicial power to declare the existence of a high-level right to privacy and I do not think that they suggest that the courts should do so*"; and *R (Catt) v Metropolitan Police Commissioner* [2015] UKSC 9, per Lord Sumption, para 2: "*The [US] concept of a legal right of privacy whether broadly or narrowly defined fell on stony ground in England. Its reception here has been relatively recent and almost entirely due to the incorporation into domestic law of the [ECHR].*"

Assembly of the Council of Europe (made up of MPs from contracting states) adopted the ECHR.

5.13. The UK was a founder member of the Council of Europe. Since 1966, it has acknowledged the right of individuals with a sufficient interest to petition the ECtHR for a ruling that it has violated their fundamental rights. Such rulings are binding upon the UK in international law,[16] and may be enforced through the political mechanisms of the Council of Europe's Committee of Ministers.[17]

5.14. Since the entry into force of the HRA 1998 in October 2000, individuals have been entitled to enforce most of their ECHR rights in domestic courts and tribunals. Those bodies are required to "*take into account*" any relevant decision of the ECtHR, and to interpret UK laws in a manner consistent with the ECHR where it is possible to do so.[18] Higher courts may also declare primary legislation (or subordinate legislation made in exercise of a power conferred by primary legislation) to be incompatible with the ECHR. Consistently with the sovereignty of Parliament, legislation is not invalidated by such a declaration. However, once appeal rights have been exhausted, the UK Government has normally been prepared to repeal or to amend legislation that has been declared incompatible by the courts.

5.15. Material provisions of the ECHR include Article 6 (right to a fair trial) and Article 10 (freedom of expression). They bear, in particular, on the treatment of lawyer-client communications and on the protection of journalists' sources, and are considered in those contexts below. But in other respects (and though the right to freedom of expression is sometimes pleaded in tandem with the right to privacy) they are generally of lesser significance than Article 8.

Article 8

5.16. Article 8 of the ECHR is headed "*Right to respect for private and family life*", sometimes rendered, in shorthand, as the "*right to privacy*".[19] It provides as follows:

> "1) Everyone has the right to respect for his private and family life, his home and correspondence;
>
> 2) There shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

---

16 ECHR, Article 46.

17 See Council of Europe, *Supervision of the execution of judgments and decisions of the ECtHR*, March 2015.

18 HRA 1998, ss2 and 3.

19 See, e.g., *Liberty v United Kingdom* (Application no. 58243/00, judgment of 1 October 2008), at para 43; *Kennedy v United Kingdom (*Application no. 26839/05, judgment of 18 May 2010) at para 179. The same convenient shorthand is used by the CJEU to describe the protections offered by Articles 7 and 8 of the EU Charter (see *Digital Rights Ireland*, paras 33-4); and cf. 2.1 above.

Article 8 (like Article 10) is a qualified right: interferences that "*engage*" Article 8 may be permitted, but only if they are in accordance with the law, pursue a legitimate aim and are necessary in a democratic society: what the ISC dubbed a "*triple test*".[20]

5.17. The ECtHR has traditionally been readier than the English courts to find that Article 8 is engaged, or engaged in more than a minor respect.[21] In the context of investigatory powers, it is engaged not only when material is read, analysed and later shared with other authorities,[22] but also when it is collected, stored and filtered, even without human intervention.[23]

5.18. Any interference must satisfy, by Article 8(2), what has been interpreted as a "*triple test*":[24] it must be ***in accordance with the law***, ***necessary in pursuit of a legitimate aim***, and ***proportionate***. The legal boundary between necessity and proportionality is not so clear as that summary suggests: both might be said to be embraced in the single phrase "*necessary in a democratic society*".[25] However, so long as all three elements are satisfied, the precise way in which they are distinguished is of secondary importance. The distinction between "*necessity*" and "*proportionality*", in the sense summarised above, is firmly embedded not only in RIPA (see, e.g. section 5(2)) but in the practices and training materials of all public authorities who apply it, and although it might be questioned as a matter of legal theory, I do not seek to disturb it in this Report.

5.19. The first element of that test is that the interference must be "***in accordance with the law****"*. In other words:

(a) the interference must have some basis in domestic law;[26]

(b) the law must be sufficiently accessible: the rules must be reasonably easy to obtain and understand;[27] and

(c) the manner in which the law will operate or be applied must be sufficiently foreseeable.

5.20. These requirements have not always proved easy to reconcile with the secret nature of electronic surveillance. A balance must be found between retaining the secrecy of operational tools and methods on the one hand, and, on the other, having a law that is "*sufficiently clear in its terms to give citizens an adequate indication as to the*

---

20 ISC Privacy and Security Report, para 23.

21 As Lord Sumption recently noted in the Supreme Court: *Catt v Association of Chief Police Officers of England Wales and Northern Ireland and others*, [2015] UKSC 9, para 26.

22 *Weber and Saravia v Germany*, (Application no. 54930/00, judgment of 26 June 2006), para 79.

23 The Supreme Court recently described it as clear that "*the state's systematic collection and storage in retrievable form even of public information about an individual is an interference with private life*": *Catt v MPC*, per Lord Sumption, para 6.

24 ISC Privacy and Security Report, paras 23-27.

25 See, e.g., *Leander v Sweden* (Application no. 9248/81, judgment of 26 March 1987) at para 58: "*the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.*"

26 *Silver and others v United Kingdom* (Application no. 5947/72, judgment of 25 March 1983), para 86.

27 *Sunday Times v United Kingdom* (Application no. 6538/74, judgment of 26 April 1979), para 49; *Silver v United Kingdom,* para 87.

circumstances in which and the conditions on which public authorities" will access their communications.[28]

5.21. The second element of the test involves the identification of a ***legitimate aim*** whose pursuit is necessary. Article 8(2) (set out at 5.16 above) provides a broad list of interests that are capable of justifying interference. The courts are almost always willing to find that a legitimate aim is being pursued, for example, national security or the prevention of crime. "*Necessary*" means less than "*indispensable*", but more than merely "*admissible*" or "*useful*". To be necessary, an interference must correspond to a "*pressing social need*".

5.22. To satisfy the third element of the test, the interference must be ***proportionate*** to the aim pursued. That is determined via a balancing exercise, which may for example require *"the interest of the … state in protecting its national security*" to be balanced against *"the seriousness of the interference with the applicant's right to respect for his private life*".[29] The ECtHR has repeatedly noted that:

(a) States have a "*margin of appreciation*" (or, in the national court, a discretionary area of judgement). However, the court is the ultimate arbiter of necessity.

(b) In order to be satisfied that the interference is proportionate, courts must be satisfied that the national law sets out sufficient safeguards against abuse, and that those safeguards have been followed in the particular case (if appropriate).[30]

5.23. The case law of the ECtHR concerning surveillance has largely focused on the first element: the requirement that any interference is "*in accordance with the law*". There is a degree of overlap between the first and third elements, particularly in respect of the procedural safeguards against abuses. As a result, there is a trend in some of the recent case law to consider those two elements together.[31]

5.24. Neither before the IPT nor in the ECtHR do those wishing to complain about a violation of their Article 8 rights have to demonstrate conclusively that their communications have been interfered with. It is enough for them to satisfy the court that it is reasonably likely that they were the subject of targeted surveillance.[32] Where bulk collection is concerned, an even more liberal test may apply.[33]

---

28 *Silver v UK,* para 88; *Malone v UK*, para 67; *Kruslin v France* (Application no. 11801/85, judgment of 24 April 1990), para 33; *Weber v Germany*, paras 93-94. For the requirement of foreseeability, in a different context, see *Khan v United Kingdom* (Application no. 35394/97, judgment of 4 October 2000). The absence of any guidelines concerning the use of listening devices in private property meant that their use was not in accordance with the law.

29 *Leander v* Sweden, para 59. For an example of a proportionality assessment in a related context, the indefinite "*blanket retention*" of suspects' fingerprints, cellular samples and DNA profiles, see *S and Marper v UK* (Application nos. 30562/04 and 30566/04, judgment of 4 December 2008), paras 118-126.

30 See *Silver v UK*, para 97; *Leander v Sweden*, paras 59-62; *Weber v Germany*, para 106.

31 See for example *Kvasnica v Slovakia* (Application no. 72094/01, judgment of 9 June 2009), para 84; and *Kennedy v UK*, para 155.

32 *Kennedy v UK*, para 123, *Stefanov v Bulgaria,* para 49.

33 *Weber v Germany*, paras 78-79; *Liberty v UK*, paras 56-57.

ECHR: specific issues

5.25. The ECtHR has considered surveillance and interception of communications on a number of occasions. In the course of those judgments, it has addressed a number of specific issues that are particularly relevant to this Review.

Distinction between content and 'communications data'

5.26. As set out in at 6.3-6.7 below, the current RIPA framework distinguishes between obtaining access to the content of communications (via interception), and the use of communications data. The majority of cases that have reached the ECtHR have concerned interception.[34] But as explained at 7.43-7.51 below, communications data play an important role in policing and counter-terrorism in the UK. Investigative agencies are often just as interested in who has been communicating with whom, and where from, as what the parties actually said to one another.

5.27. The Strasbourg case law is clear that both the collection of communications data and the interception of content interfere with Article 8.[35] In some cases, there are hints in the ECtHR jurisprudence that they may legitimately be treated differently. In *Malone v UK* the Applicant complained that his phone calls were not only being recorded but metered, in the sense that records were being kept regarding to whom he had spoken and when. The ECtHR commented that:

> "By its very nature, metering is … to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified..." (para 84).[36]

5.28. However, more recent cases do not appear to follow such a distinction, and it at least appears that in some circumstances the difference is of no significance. In the Liberty IPT case, the IPT referred to six principles set out below (from *Weber v Germany*) and concluded that they should apply to both kinds of material:

> "In the case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power (1) the nature of the offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their telephones tapped; (3) a limit on the duration of telephone tapping; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which recordings may or must be erased or the tapes destroyed."[37]

---

34 See for example *Malone v UK; Weber v Germany; Liberty v UK; Kennedy v UK.*

35 *Malone v UK*, para 84; *Copland v United Kingdom* (Application no. 62617/00, judgment of 03 April 2007), paras 39-47.

36 Cf. *Uzun v Germany* (Application no. 35623/05, judgment of 2 September 2010), in which the "*rather strict standards*" applicable to the interception of telephone conversations were held not to apply to the placing of a GPS tracking device in a car, para 66.

37 *Weber v Germany* para 95, cited in the Liberty IPT case, judgment of 5 December 2014, para 114.

5.29. It seems therefore that the authorisation, storage and use of communications data and of intercepted material must each meet the *Weber v Germany* standard. That is consistent with the detailed picture of an individual's life that can be obtained from communications data, particularly when different sources are combined.[38]

5.30. Where the same kind of material is gathered via different means, distinctions may be particularly hard to draw. In *Bykov v Russia*, the Grand Chamber of the ECtHR held that the bugging of a live conversation in a sting operation attracted the same protections as interception of communications.[39]

Bulk collection

5.31. Bulk collection of both communications data and intercepted material has been one of the leading sources of controversy following the disclosure of the Snowden Documents. Bulk collection is potentially problematic, from an ECHR perspective, because of the sheer number of individuals whose private lives are interfered with. As a result, and leaving aside the question of whether it is in accordance with the law, it may be more difficult to demonstrate that the interference is "*necessary in a democratic society"*, or proportionate.

5.32. Most applicants to the ECtHR focus on the individual alleged violations of their right to privacy.[40] The court has only considered bulk collection on a small number of occasions. The leading authority in this area is *Weber v Germany*, in which the applicants complained that the German state was monitoring communications in the absence of any "*concrete suspicion*" and relying on "*catchwords*" in order to analyse the data. The ECtHR dismissed the application as manifestly ill-founded, noting (at paras 114-117) that "*strategic monitoring*" was not in itself a disproportionate interference with the right to privacy. In so concluding it had regard to the narrow and closely defined justifications for such collection, the safeguards that governed the authorisation of the collection, the safeguards concerning use of that material and the data protection systems in place.

5.33. In the other leading case concerning bulk collection of intercepted material, *Liberty v UK*, the court concluded that the UK legislation in question (the Interception of Communications Act 1985 **[IOCA 1985]**) was not in accordance with the law. IOCA 1985 did not provide sufficient safeguards against abuse of the power to intercept or use the material in question.[41] Because the case was decided on the "*in accordance with the law*" basis, the court did not explicitly consider whether the interference in question was proportionate. On the other hand, as set out above, the court frequently

38 As the CJEU recently explained in *Digital Rights Ireland,* para 26: "*Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*."

39 Application no. 4378/02, judgment of 10 March 2009, paras 78-79.

40 See for example the judgment in *Kennedy v UK*, which considered the lawfulness of the s8(1) framework for individualised warrants but not the more general powers under s8(4).

41 *Liberty v UK*, para 69.

considers very similar factors under the headings of "*in accordance with the law*" and proportionality (and may even consider them together).

5.34. In summary, the case law of the ECtHR suggests that bulk data collection and analysis, in the absence of suspicion, is not in itself a disproportionate interference with the right to respect for private life. However, bulk collection will be assessed against a higher standard than individual interferences with the right to privacy. The justification for that interference, and the safeguards in place to prevent abuse, will need to be more compelling if the requirements of Article 8(2) are to be satisfied.[42]

5.35. The IPT recently heard extensive argument concerning whether or not the current bulk interception processes under RIPA s8(4) were "*in accordance with the law*" in the Liberty IPT Case. The Claimants argued that the current distinction between internal and external communication was so unclear that the bulk collection framework was itself unlawful. They also argued that data sharing arrangements between various governments and the UK were not in accordance with the law, and that insufficient safeguards were in place. All those arguments were rejected in the judgment of 5 December 2014, though the IPT went on to rule that prior to disclosures made in 2014, the regime for sharing data with the US had contravened the "*in accordance with the law*" requirement.[43] After further (closed) argument, the IPT is expected to determine the Claimants' submissions that the bulk interception of external communications is a disproportionate interference with their Article 8 and Article 10 rights. The Claimants have already applied to the ECtHR in relation to the arguments rejected by the IPT.[44]

Home and away

5.36. Every state of whose legal framework I am aware draws some kind of distinction between the protections afforded to its own citizens or residents and others.[45] The apparent distinction in RIPA between "*internal"* and "*external*" communications, together with the additional safeguards under RIPA s16 for persons known to be for the time being in the British Islands,[46] is explained at 6.42-6.59 below.

5.37. The ECHR case law has not directly considered the lawfulness of that dichotomy. [47] As a general rule, Member States do not owe ECHR duties to individuals outside their territory or "*effective control*".[48] However, both the case law of the ECtHR and the UN Human Rights Committee have made clear that treaty obligations may extend extraterritorially.[49] The application of that doctrine to surveillance conducted abroad

---

42 That conclusion is consistent with the approach adopted by the CJEU in *Digital Rights Ireland* as set out below.

43 Liberty IPT Case, judgment of 6 February 2015.

44 *10 Human Rights Organisations v United Kingdom,* an application filed on 10 April 2015 **[Liberty ECtHR Application]**.

45 See further 5.90 and 14.76-14.77 below.

46 British Islands means the UK, Channel Islands and Isle of Man: Interpetation Act 1978 s5.

47 In *Weber v Germany*, the ECtHR declined to decide the question of whether German nationals resident in Uruguay who complained of "s*trategic monitoring*" of international telecommunications by the German Federal Intelligence Service were entitled to the protection of the ECHR (the case being declared inadmissible on other grounds).

48 In *Al Skeini v United Kingdom* (Application no. 55721/07, judgment of 7 July 2011), paras 138-148.

49 European Commission for Democracy Through Law (Venice Commission), *Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies*, Study No 719/2013, April 2015, **[Venice Commission Report]**, paras 69-71.

is uncertain, but some possibilities were recently alluded to by the Venice Commission of the Council of Europe:

> "The collection of intelligence on or over the high seas, or in the territory of another state, with that state's permission, will not be in violation of the customary international law norm of non-intervention. However ... [c]ollection facilities in military bases, or vessels situated outside national territory, can … be within '*jurisdiction*' for state parties to [the ECHR]. In any event, the processing, analysis and communication of this material is clearly within national jurisdiction and is governed both by national law and states' applicable human rights obligations."[50]

5.38. For practical purposes, it is likely that any framework for the interception of external communications, however defined, will have to be ECHR-compliant. It is generally acknowledged to be impossible, when gathering communications between two individuals who are both outside the UK, to avoid collecting some communications that are internal, in the sense that they are both to and from individuals inside the British Islands.[51]

5.39. Jurisdictional issues arise also in relation to the extra-territorial application of national laws requiring overseas service providers to make data available (e.g. DRIPA 2014 s4), particularly where those laws come into conflict with data protection requirements in the foreign state. As suggested by the Venice Commission, the long-term resolution of this issue may require new international standards for privacy.[52]

Oversight and authorisation

5.40. The ECtHR has repeatedly affirmed that:

> "...in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge."[53]

5.41. However, in *Klass v Germany* it rejected the submission that authorisation must be provided by a judge. The ECtHR explained that review of surveillance may take place at three stages: when the surveillance is first authorised, while it is being carried out and after it has been terminated. The initial authorisation process in Germany was made by the relevant minister or law enforcement officer (much like the current system in the UK). The implementation of the measure was overseen by an official qualified for judicial office. The material that was gathered did not go direct to the competent authorities: rather it was reviewed by that official to determine whether its use was compatible with the relevant legislation. Review after the event was carried out by

---

See also *Al-Jedda v UK* (Application no. 27021/08, Judgment of 7 July 2011) and UN Special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 4th annual report, 23 September 2014 (A/69/397).

50 *Ibid.,* para 69.

51 See 6.53 below.

52 Venice Commission Report, para 71.

53 *Klass v Germany* (Application no. 5029/71, judgment of 6 September 1978), para 56; *Kruslin v France*, para 34; *Kennedy v UK*, para 167.

two bodies, a Parliamentary Control Commission and the G10 Commission, both of which were independent of the authorities carrying out the surveillance and contained members of the opposition parties.[54] The court reviewed all aspects of the authorisation and oversight regime and concluded it provided sufficient protections to democratic freedoms.

5.42. The current system of ministerial authorisation for individual warrants does not render the system non-compliant with Article 8, in the opinion of the ECtHR. In *Kennedy v UK*, the ECtHR explained in detail the oversight that is currently provided by the IOCC, the ISC and the IPT.[55] The court did not set out a standard of oversight and then ask whether or not the current framework meets that test. Rather the strength of the oversight regime was one factor that it took into account when determining whether the RIPA s8(1) framework was a necessary and proportionate and interference with the right to privacy; and the absence of judicial involvement during the authorisation or implementation stage was not fatal.

5.43. It should be noted that the *Kennedy* case concerned individual warrants rather than bulk collection.

Confidential communications

5.44. Certain kinds of communication deserve particular protection, and need to be approached with especial care.

5.45. First, communications between lawyers and their clients are protected by ***legal professional privilege*** **[LPP]**.[56] Similar or equivalent provisions exist in the laws of most other European countries.[57] The ECtHR has held that, where a search warrant is executed at a lawyer's office, "*special procedural safeguards, such as the presence of an independent observer*" should be put in place to avoid an unwarranted breach of professional confidence.[58]

5.46. The same principles will apply in cases concerning interception of material subject to LPP. The precise scope of the additional and further protections that should apply when privileged documents are being intercepted has not been fully argued in any case before the ECtHR.[59] However, it is clear that such protections are required:

(a) In *Kopp v Switzerland* the Swiss authorities had tapped the telephones of a law firm, as part of a wider investigation into corruption. The ECtHR held that was not in accordance with the law, because Swiss law failed clearly and adequately

54 They were held to be sufficiently independent "*to give an objective ruling*", *Klass v Germany*, para 56.

55 *Kennedy v UK*, paras 166-9.

56 Whether communications data (recording, for example, the fact that a lawyer spoke to a client or a potential witness) may be subject to LPP is not entirely straightforward: see *JSC Bank v Ablyazov Bank* [2012] EWHC 1252 Comm; C. Hollander, *Documentary Evidence* (12th edn., 2015) para 17-29. The fact of such communications is presumably confidential, in any event, and likely to be of special sensitivity: *IOCCO inquiry into the use of RIPA Part I Chapter 2 to identify journalistic sources,* (February 2015), para 6.16.

57 *R (Prudential) v Special Commissioner of Income Tax* [2013] UKSC 13, paras 116 and 136.

58 *Niemietz v Germany*, para 37. See also *Stefanov v Bulgaria*, para 38.

59 As noted at 5.68(b) below, the CJEU, when determining that the Data Retention Directive was not lawful, also noted that it made no provision for communications that are subject to professional secrecy (*Digital Rights Ireland*, at para 58).

to distinguish between those communications that would attract privilege and those that would not. The court was also particularly exercised that the determination of that question was delegated to an official in the Post Office's legal department: a part of the executive and not an independent judge.[60]

(b) In other cases, the court has noted with approval that the French state offered specific protections to preserve the confidentiality of lawyer/client relations when their telephones are to be tapped.[61] Additional protections will also be necessary, in many cases, in order to protect the right under ECHR Article 6 to a right to a fair trial.[62]

5.47. In the domestic sphere, the Judicial Committee of the House of Lords (the predecessor body to the UK Supreme Court) considered the question of LPP in the context of surveillance. The case concerned the power to listen in to confidential consultations held at a police station between lawyers or doctors and their clients. The court held that it was lawful, in some circumstances and where authorised expressly by statute, to carry out surveillance of those conversations. However, the House of Lords also upheld the view of the Administrative Court that the safeguards set out in RIPA, and the Code of Practice for surveillance, offered insufficient protections in a case where privileged communications would be gathered.[63]

5.48. More light has recently been shed on this issue by the Belhadj IPT case. The UK Government had already conceded that its policy concerning interception of privileged communications has been unlawful: the IPT held that the privileged communications of a claimant had been intercepted, and ordered GCHQ to destroy its copies of the relevant documents.[64] Both the Draft Interception of Communications Code of Practice of February 2015 **[Draft Interception Code]** and the new Acquisition and Disclosure of Communications Data Code of March 2015 **[Acquisition Code]** contain expanded sections concerning access to privileged communications.[65]

5.49. Secondly, communications between ***journalists and their sources*** are entitled to be treated in confidence. The ECtHR has held that an interference with the confidentiality of journalistic sources can only be justified by "*an overriding requirement in the public interest.*"[66] The threshold that must be passed is significantly higher than the ordinary necessity and proportionality test. In *Weber v Germany* the applicant was a journalist, who argued that the interception of her communications was a breach of her right to maintain the confidentiality of her sources. The ECtHR held that the purpose of "*strategic monitoring*" (widespread and without reference to a particular individual) was not to gather information about journalistic sources. Therefore, the procedures

60 *Kopp v Switzerland* (Application no. 13/1997, judgment of 25 March1998), paras 73-75.
61 *Kruslin v France,* para 34; *Huvig v France* (Application no. 11105/84, judgment of 24 April 1990), para 33.
62 See *S v Switzerland* (Application no. 12629/87, judgment of 28 November 1991).
63 *McE v Prison Service of Northern Ireland and another, C and Another v Chief Constable of the Police Service of Northern Ireland and M v Same* [2009] UKHL 15, [2009] 1 AC 908. See in particular the comments of Lord Neuberger, para 113.
64 Belhadj IPT Case, order of 26 February 2015; judgment of 29 April 2015. The decision was the first time the IPT has found in favour of an individual Claimant, in an open judgment, and held that the Agencies have acted unlawfully.
65 Draft Interception Code paras 4.2-4.25; Acquisition Code paras 3.72-3.84.
66 *Goodwin v United Kingdom* (Application no. 17488, judgment of 27 March 1996), para 39.

that were in place to restrict the use and dissemination of material were sufficient to protect journalists' freedom of expression and the confidentiality of their sources.[67]

5.50. However, in a Dutch case the ECtHR held that two investigative journalists had suffered a disproportionate interference with their right to privacy as a result of covert surveillance. In that case, the purpose of the surveillance was to identify a journalistic source and there was insufficient judicial oversight to render the intervention legal.[68] That conclusion was echoed in a subsequent case. The ECtHR stressed that special safeguards must be in place in order to protect the confidentiality of journalistic sources, stating: "*First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body*."[69]

5.51. The Bureau of Investigative Journalism has issued proceedings before the ECtHR arguing that the current protections provided under UK law do not afford sufficient protection to journalists' sources.[70] The matter has been communicated to the Government. Meanwhile another challenge has been filed in the IPT by a Sun journalist, concerning access to his phone records.[71]

5.52. A third category of protected communications, which has not been considered by the ECtHR, is ***parliamentary correspondence***. A claim has been issued before the IPT concerning the interception of communications to and from Parliamentarians.[72] A hearing on preliminary issues of law will take place in July 2015.

5.53. Other communications may be specifically protected. The ECtHR has also held that medical information attracts the protection of Article 8. In *Z v Finland*, the fact that the applicant was HIV positive was disclosed in the press reporting of her trial. The court held that her right to respect for private life had been breached.[73]

Pending cases before the ECtHR

5.54. The case of *Big Brother Watch v UK* was lodged before the ECtHR in 2013,[74] and communicated to the UK Government. It concerns bulk data collection and data sharing. In addition, the Liberty ECtHR Application (5.35 above) and the application brought by the Bureau of Investigative Journalists (5.51 above) have been communicated to the UK Government.

---

67 *Weber v Germany*, paras 150-152.

68 *Telegraaf Media Nederland Landelijke Media BV and others v The Netherlands* (Application no. 39315/06, judgment of 22 November 2012), paras 96-102.

69 *Sanoma Uitgevers BV v The Netherland (*Application no. 38224/03, judgment of 14 September 2010), para 90.

70 *Bureau of Investigative Journalism and Alice Ross v UK* (Application no. 62322/14). The current Interception of Communications Code of Practice **[Interception Code]** sets out some safeguards at sections 3.2, 3.6 and 3.9.

71 No record of the case number is available on the IPT website yet.

72 *Lucas and Moulsecoomb v the Security Service and others* (IPT/14/79/CH and 14/80CH). It has recently been joined with a similar claim issued by George Galloway MP.

73 *Z v Finland* (Application no. 22009/93, judgment of 25 March 1997).

74 Application no. 58170/13.

The law of the European Union

5.55. The UK is a Member State of the EU, an international organisation governed by treaties. Parliament has given primacy to EU law, as EU law itself demands.[75] Although the EU is not itself a signatory to the ECHR,[76] it has its own system of rights protection which, within the scope of the Treaties, constrains the legislative freedom both of the Union and of its Member States.

5.56. The legal acts of the EU[77] may be annulled or declared invalid if they are inconsistent with the EU Treaties, with the fundamental rights which constitute "*general principles of the Union's law*"[78] or with the EU Charter, which has the same legal value as the Treaties.[79] Furthermore, unlike under the ECHR, both the CJEU and domestic courts are obliged to "*disapply*" provisions of national law, including Acts of Parliament, that conflict with EU legal norms. In contrast to the ECtHR's political enforcement mechanisms, Member States which fail to rectify an infringement determined by the CJEU are liable to be heavily fined.[80]

Charter of Fundamental Rights

5.57. Of particular relevance to the law on investigatory powers are Articles 7 and 8 of the EU Charter, which are based on the ECHR and read as follows:

> "Article 7: Respect for private and family life
>
> Everyone has the right to respect for his or her private and family life, home and communications.
>
> Article 8: Protection of personal data.
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority."

---

75 ECA 1972, ss2 and 3.

76 It is obliged to accede to the ECHR (TEU Article 6(2)); but that prospect is not imminent: Opinion of the CJEU 2/13, 18 December 2014 EU:C:2014:2454.

77 Such legal acts include regulations (which are binding in their entirety and directly applicable) and directives (which need to be implemented in national law, but are binding as to the result to be achieved): TEU, Articles 288 and 289.

78 TEU, Article 6(3).

79 TEU, Article 6(1).

80 Treaty on the Functioning of the European Union, Article 260.

5.58. There is no direct equivalent in the EU Charter of Article 8(2) of the ECHR. But Article 52(1) provides that:

> "Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others,"

and the "*objectives of general interest*" are effectively limited to those referred to in Article 8(2) of the ECHR by Article 52(3), which provides that insofar as the EU Charter rights correspond with ECHR rights, "*the meaning and scope of those rights shall be the same*". That is to be read however together with the last sentence of Article 52(3): "*This provision shall not prevent Union law providing more extensive protection*". The position is thus that the ECHR provides a floor for interpreting the EU Charter rights, but not a ceiling.

Data protection law

5.59. Two pieces of EU legislation constrain the freedom to gather and process information without constraint, via surveillance or any other method.[81]

5.60. First, the Data Protection Directive sets out a framework for "*data processing*" that respects "*fundamental rights and freedoms, notably the right to privac12 y*" (Recital 2). It lays out the standards that govern the processing of personal data, including the collection, recording, organisation, storage, adaptation, retrieval, consultation, use or dissemination of that material throughout the Union (Article 2). Personal data may only be collected for "*specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes"* (Article 6(1)(b)) and "*kept in a form which permits identification of data subject for no longer than is necessary for the purposes for which the data were collected...*" (Article 6(1)(e)).[82]

5.61. Member States are obliged to ensure that appropriate technical and organisational measures are in place to protect personal data from accidental or unlawful destruction, loss or unauthorised disclosure (Article 17(1)).

5.62. Secondly, the e-Privacy Directive is concerned with the data generated by and in association with use of electronic communications. It harmonises the standards of protection throughout Europe, in order to ensure that personal data, which is protected by Articles 7 and 8 of the EU Charter, is given adequate security. Article 15(1) provides:[83]

> "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4) and Article 9 of this Directive, when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the

81 Though it is arguable that they do not do so in all circumstances: see, in particular, the comments on TEU Article 4(2) at 5.2(b) above.

82 Directive 95/46/EC.

83 Directive 2002/58/EC.

prevention, investigation, detection and prosecution of criminal offences ... To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph."

Digital Rights Ireland

5.63. The CJEU has had, until recently, less opportunity than the ECtHR to pronounce upon the law of investigatory powers.[84] But as the court entrusted with the interpretation of the EU Charter, a document which has the potential to be construed in a more expansive manner than the ECHR, its judgments in this area may prove in the long run to be at least as significant.

5.64. Of particular importance is the judgment of the Grand Chamber of the CJEU in *Digital Rights Ireland*, a successful challenge to the validity of the EU's Data Retention Directive.[85]

5.65. The EU Data Retention Directive, harmonising the various responses by Member States to Article 15(1) of the e-Privacy Directive, required service providers to retain data generated for billing purposes concerning use of telephone, internet and email services for between six and 24 months. The scope of the data in question was broad and included data necessary to identify a sender and recipient, date, time and duration, type, equipment of communication and the location of mobile phone calls. Those data were to be held, beyond the period of time when a service provider might need them, in order to assist in the investigation and prevention of serious crime. The service provider was required to make data available, on request, to the police and security services. The implementing legislation in the UK required service providers to keep that data for 12 months.[86]

5.66. Largely uncontroversial in the UK, the Data Retention Directive evoked strong feelings in other parts of Europe, culminating in the presentation of mass petitions and a number of constitutional challenges to its implementation.[87]

5.67. The CJEU acknowledged that data retained under the Directive could be valuable. Thus:

(a) It noted "*the growing importance of means of electronic communication*", and described data retained under the Directive as "*a valuable tool for criminal investigations*" which afforded the authorities "*additional opportunities to shed light on serious crime*".

(b) The fight against serious crime, "*in particular against organised crime and terrorism*", was itself described as "*of the utmost importance in order to ensure*

84 Though see Joined Cases 46/87 and 227/88 *Hoechst AG v Commission* EU:C:1989:337 (law of search) and Case C-550/07P *Akzo Nobel v Commission* EU:C:2010:512 (legal professional privilege).

85 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* and *Seitlinger and others* ECLI:EU:C:2014:238.

86 The Data Retention (EC Directive) Regulations 2009 (SI 859/2009) s5.

87 See 8.56-8.57 below.

public security", and as potentially dependent for its effectiveness on "*the use of modern investigation techniques*".[88]

5.68. This notwithstanding, the CJEU declared the Data Retention Directive to be invalid, for failure to comply with the principle of proportionality. The utility of the Directive in the fight against serious crime was not enough to render it "*necessary"*, in the absence of safeguards which the court ruled that the EU legislator should have provided. In particular:

(a) The Directive mandated the ***bulk retention*** of "*all traffic data*" relating to "*all means of electronic communication*" used by "*practically the entire European population*", including those in respect of whom there was no suggestion that they had a connection, even indirect or remote, with serious crime (paras 56-58).

(b) The Directive did not allow for any exceptions relating to communications that are subject to ***professional secrecy*** (para 58).

(c) The Directive did not require any "*relationship between the data whose retention is provided for and a threat to national security*": in particular, ***retention was not restricted*** by reference to particular time periods, places or persons who were likely to be involved in serious crime or who could contribute to its prevention, detection or prosecution (para 59).

(d) The Directive did not lay down "*any objective criterion*" by which to determine the ***types of "serious crime***" in respect of which the retained data could be accessed or used: deferring to national definitions was not enough (para 60).

(e) The Directive contained no substantive or procedural conditions concerning ***access to and use of the data***. In particular, it did not restrict access and use of the data to what is strictly necessary for "*preventing and detecting precisely defined serious offences or conducting criminal prosecutions relating thereto*" (para 61).

(f) The Directive did not lay down objective criteria to limit the number of persons authorised to access and use retained data. "*Above all*", access by national authorities was not made dependent on a "***prior review*** *carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary...*" (para 62).

(g) The Directive required all data without distinction to be retained for at least six months, and did not ensure that ***retention periods*** must be limited to what is strictly necessary (paras 63-64).

(h) The Directive did not provide for sufficient ***protection and security*** against abuse and unlawful access, bearing in mind the "*vast quantity*" and "*sensitive nature*" of the data. Service providers were wrongly allowed to have regard to

88 *Digital Rights Ireland*, paras 49 and 51.

economic considerations when determining the level of security which they applied and the Directive did not ensure the "*irreversible destruction*" of the data at the end of the data retention period (paras 66-67).

(i) The Directive did not require that the data be ***retained within the EU***, contrary to the requirement of Article 8(3) of the EU Charter that compliance with the data protection rules envisaged in Article 8 be controlled by an independent authority (para 68).

Consequences of Digital Rights Ireland

5.69. The precise boundaries of the judgment will not be established for some time. Some have construed it as an attack on the whole notion of bulk data retention.[89] From another perspective, the UK Government has suggested to me that the CJEU did not hear detailed argument on some of the requirements that it referred to in its judgment; and that it is not entirely clear whether each of the grounds summarised at 5.68 above would have been sufficient to invalidate the Data Retention Directive, or whether it is only their cumulative effect that did so.

Dutch case

5.70. The District Court of the Hague, in judgment of March 2015, recently struck down the Dutch data retention legislation.[90] The judgment is of course not binding in the UK. But as an interpretation by a national court of the CJEU's binding *Digital Rights Ireland* judgment, it deserves careful study.

5.71. Although the Dutch law was described as "*autonomous legislation that should be assessed on its own merits*", it was subject to the constraints of the EU Charter, as interpreted in *Digital Rights Ireland*, because Member States which legislate for data retention are both implementing the e-Privacy Directive and restricting the free movement of services. The same conclusion is likely in the UK context.[91]

5.72. The District Court rendered the Dutch law inoperable, notwithstanding the State's unchallenged submissions that "*the detection of certain types of crimes rely almost exclusively on the use of historical telecommunication data*" and that "*some of its*

89 See F. Fabbrini, "Human Rights in the Digital Age. The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the US", (2014) Tilburg Law School Legal Studies Research Paper Series (15), para 24: **"***De facto it rules out anything short of individualised, court-approved, requests by national security and law enforcement authorities to collect and use meta-data generated in electronic communications for specific searches."* See also the extra-judicial comments of the *juge rapporteur* (the member of the CJEU responsible for preparing the judgment), Thomas von Danwitz, in an interview with the Süddeutsche Zeitung on 17 September 2014: "Q. *So would the general retention of communications data without cause no longer be admissible following the ruling? A. That is certainly the essence of the ruling, and so a provision introducing a general obligation to retain, without any grounds for suspicion, would be problematic.*"

90 NL:RBDHA:2015:2498, District Court of the Hague, 11 March 2015, Case no. C/09/480009/KG/ZA 14/1575 (unofficial translation by Anna Berlee for the Interdisciplinary Internet Institute). Other national data retention laws have also been annulled since the *Digital Rights Ireland* judgment: see 8.56-8.57 below.

91 The notion of a "*UK opt-out*" from the EU Charter was always a misconception. See my written evidence to the EU Scrutiny Committee in January 2014, at paras 5-10: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/european-scrutiny-committee/the-application-of-the-eu-charter-of-fundamental-rights-in-the-uk/written/4922.html.

extensive criminal cases could not have been resolved without data retention". It indeed recognised that its judgment "*may have profound implications for the detection and prosecution of offences*" (para 3.6).

5.73. As to the detail, the District Court construed the *Digital Rights Ireland* criteria, summarised at 5.68 above, as having contributed collectively to the CJEU's conclusions. This was helpful to the State, for it enabled the District Court to find unobjectionable the fact that the Dutch law provided for the storage of everybody's data, and not just those of suspected criminals (5.68(a) and (c), above). The court pointed out that a limitation such as that apparently envisaged by the CJEU would not be conceivable in view of the law's purpose of tracing serious crime: "*Indeed, in the case of a first offender, it is not possible to make a distinction in advance between suspect and non-suspect citizens*".

5.74. Other features of the Dutch law however rendered it disproportionate, having regard to *Digital Rights Ireland*, in particular:

(a) its failure to provide that the data should be retained within the EU, which was described as "*an essential component for the protection of the people in the processing of personal data*" (cf 5.68(i) above), and

(b) the fact that retained data could be used in relation to "*criminal offences not sufficiently serious to justify the interference*", including bicycle theft and (it would appear) all other offences for which a suspect could be remanded in custody: cf. 5.68(e) above.[92]

These matters were said to be all the more important because access to the retained data did not require prior authorisation by a judicial authority or independent administrative body: 5.68(f)5.68 above. [93]

English case

5.75. The equivalent UK case is a judicial review claim by two Members of Parliament (Tom Watson MP and David Davis MP) challenging DRIPA 2014, s1, on the grounds that it is inconsistent with *Digital Rights Ireland*.[94] That case was given permission by the Administrative Court to proceed, and is currently listed for hearing in June 2015.

The future

5.76. Only the courts (and ultimately, the CJEU) can pronounce authoritatively on the extent to which *Digital Rights Ireland* constrains current and future UK data retention rules. If the EU adopts a replacement Data Retention Directive, which it may do in the future, that too will serve as a constraint. But even if (to make assumptions favourable to the Government) the Directive turns out to have been invalidated only on the basis of the *cumulative* application of the factors set out at 5.68 above, and even if the Dutch court

92 The District Court noted in this regard that the Data Retention Directive was a response to the terror attacks in Madrid and London of 2004-2005.

93 Paras 3.9-3.11.

94 *David Davis MP and Tom Watson MP v Home Secretary*.

is correct that to limit the categories of person whose data is retained, as the CJEU appears to have wished, would be to destroy the whole concept of data retention and cannot therefore have been intended, the *Digital Rights Ireland* constraints will still be significant. To pass muster under EU law, the UK rules that replace DRIPA 2014 s1 and the Data Retention Regulations 2014/2042 will have to be prefaced at the very least by consideration of:

(a) limiting the use of retained data to specified categories of "*serious crime*";

(b) substantive and procedural conditions for access to and use of retained data;

(c) prior authorisation by a judicial authority or independent administrative body;

(d) variable retention periods, limited to what is strictly necessary;

(e) provision for the physical security of data and its irreversible destruction when the retention period ends;

(f) special treatment for communications subject to professional secrecy; and

(g) the retention of data within the EU.

5.77. The Grand Chamber of the CJEU is the apex of the judicial pyramid where EU law is concerned, and its conclusions are strictly binding. The extent to which current UK law gives effect to the requirements of *Digital Rights Ireland* is disputed in the MPs' case referred to at 5.75 above, which will be heard in the High Court in June 2015. In the circumstances, it would be inappropriate for me to venture an opinion on its legal compatibility.

5.78. There are however powerful arguments against an over-broad interpretation of the *Digital Rights Ireland* judgment. In particular:

(a) What the Grand Chamber said about prior independent authorisation (5.68(f), above), seems to go further than the case law of the ECtHR but without explaining why. See, for example, *Kennedy v UK* (not cited by the Grand Chamber), in which the ECtHR accepted prior authorisation of individual warrants by the Secretary of State even where the interception of content was concerned.

(b) Though the CJEU was prepared to describe data retention as a "*particularly serious*" infringement of fundamental rights, concrete examples of harm are not provided and are not immediately evident.[95] While there may be some for whom the retention of data "*is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant*

[95] The CJEU's suggestion that "*it is not inconceivable that the retention of the data in question might have an effect on the use … of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression*" (*Digital Rights Ireland*, para 28) appears tentative and largely theoretical, at least where law-abiding people falling outside the specially protected categories are concerned.

surveillance" (*Digital Rights Ireland*, para 37), the survey evidence suggests that this is putting it rather high.[96]

(c) There is a case for excluding the use of retained communications data in relation to the most trivial of offences (5.67(e) above). But if the mark for "*serious crime*" is set too high, damaging crimes will go needlessly unpunished and public confidence in law enforcement will be reduced.

(d) To limit retention to "*particular persons likely to be involved, in one way or another, in a serious crime*", and/or to "*persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences*" (*Digital Rights Ireland*, para 59), would not only reduce the effectiveness of data retention in identifying targets but would carry other risks, since to seek to apply such nebulous distinctions would be to court allegations of prejudice, profiling and unlawful discrimination.[97]

5.79. The wider implications of the judgment also need to be reflected upon. Though *Digital Rights Ireland* did not concern the bulk interception of content, it is arguable that its principles (including in relation to prior independent authorisation) should apply in that area with at least the same force.[98] Indeed the CJEU stated in terms that the bulk interception of content would be more intrusive, since unlike the Data Retention Directive it would affect the "*essence*" of the fundamental right to privacy (para 39). There may be implications also for other types of surveillance in relation to which types of self-authorisation are practised, in particular by the security and intelligence agencies. All this is subject to EU law being applicable: though to the extent that *Digital Rights Ireland* may in the future be adopted or followed by the ECtHR, that distinction will cease to matter.

Google Spain

5.80. A further, more recent decision that may also affect any future data retention legislation is the judgment in Case C-131/12 *Google v Spain*.[99] The CJEU determined, in brief, that a search engine (such as Google) was a data controller for the purposes of the Data Retention Directive. As a result, it was obliged to protect the fundamental rights of the owner of that data and in particular to protect the right to be "*forgotten*" by responding to requests that certain data be destroyed or not made available.

---

96 See, e.g., TNS-BMRB (2.27(a) above).

97 My experience as independent reviewer of terrorism legislation indicates that the universal exercise of intrusive powers (e.g. to require screening at an airport) is accepted by almost everybody, whereas the use of discretionary intrusive powers (stop and search; port detentions) may be perceived as discriminatory and used (whether justifiably or not) to foment a sense of grievance in affected communities.

98 Note however that the point is currently in dispute before the courts; and that it was ruled in the Liberty IPT case (though by reference only to ECHR case law) that the existing UK system for authorising interception warrants is unobjectionable: Liberty IPT Case, judgment of 5 December 2014, para 116(vi).

99 EU:C:2014:317.

5.81. Following *Google v Spain,* service providers and government agencies that hold communications data, are data controllers. They should be prepared to receive, and where appropriate agree, to requests for data destruction.

Pending cases before the CJEU

5.82. Two other cases, though not yet decided by the CJEU, should be mentioned:

(a) the case referred by the Irish High Court regarding the adequacy of the "*safe harbour*" agreement under which data is transferred in bulk to companies such as Facebook, where it is subject to less onerous data protection rules than in the EU;[100] and

(b) the pending opinion on the lawfulness of the EU-Canada agreement on sharing air passenger data in bulk, referred to the CJEU by the European Parliament on 25 November 2014.[101]

5.83. Both may shed further light on the attitude of the CJEU towards the sharing of bulk data.

International Law

5.84. Principles of international law (with the exception of customary international law) cannot generally be relied upon in the UK courts unless they have been incorporated into UK domestic legislation.[102] Treaty obligations are binding as a matter of international law; but the jurisprudence of public international law is less complete than that of the European courts, and adds little to it.

5.85. Nonetheless, the reports of UN High Commissioners and Special Rapporteurs command respect, and may in the future be influential in establishing international norms.

Treaty law

5.86. The principal relevant Treaty provision is Article 17 of the International Covenant on Civil and Political Rights 1966 **[ICCPR]**:

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

100 Case C-362/14 *Schrems v Data Protection Commissioner*.

101 https://edri.org/eu-canada-agreement-on-pnr-referred-to-the-cjeu-whats-next/. For EU law on data surveillance and sharing, see C. Murphy, *EU Counter-Terrorism Law* (2012), chapter 6.

102 *R (SG and others) v Secretary of State for Work and Pensions* [2015] UKSC 16, per Lord Reed at para 90. In an interesting dissenting opinion, Lord Kerr at paras 235-257 challenged this "*constitutional orthodoxy*" on the basis that "*If the government commits itself to a standard of human rights protection, it seems to me entirely logical that it should be held to account in the courts as to its actual compliance with that standard*".

> 2. Everyone has the right to the protection of the law against such interference or attacks."

The ICCPR was referred to in the recent report of Ben Emmerson QC: 5.91 below.

UN High Commissioner for Human Rights

5.87. In December 2013, the General Assembly of the United Nations adopted Resolution 68/167 concerning the right to privacy in the digital age. It notes that "*unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data* [are] *highly intrusive acts* [that] *violate the rights to privacy and to freedom of expression and may contradict the tenets of a democratic society*." The Resolution calls on states to act in accordance with international law and to establish effective oversight, to respect the right to privacy and to review their current mechanisms of surveillance.

5.88. The Resolution requested the UN High Commissioner for Human Rights, Ms Navanethem Pillay, to submit a report on the protection and promotion of the right to privacy. That Report, was published on 30 June 2014.[103] Drawing on the work of the Human Rights Committee, the Commissioner stated, in language familiar from the European case law:

> "Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed."

She went on to apply that reasoning to what she called mass or bulk surveillance programmes, pointing out (para 25) that:

> "... it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate."

UN Special Rapporteur

5.89. The UN Special Rapporteur on the promotion and protection of fundamental rights and human freedoms while countering terrorism, Ben Emmerson QC, wrote about the subject in his fourth annual report in September 2014.[104] He stated that "*the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether",* and argued (at paras 12-14) that given the scale of the interference with privacy, the corresponding public policy benefit must be very substantial.

5.90. He also suggested (at paras 42-43) that laws which distinguish between internal and external communications, either by reference to physical location as in the UK or

103 *The right to privacy in the digital age*, (June 2014), A/HRC/37.
104 A/69/397.

citizenship as in the United States, are unlawful. He stated that Article 26 of the ICCPR, prohibiting discrimination, requires all States "*to afford the same privacy protection for nationals and non-nationals and for those within and outside their jurisdiction*" (para 62). If so, the ICCPR may impose more onerous obligations than the ECHR, which protects only those within the jurisdiction of its contracting States, including areas outside their borders over which they have effective control.

5.91. Both the Human Rights Commissioner and the Special Rapporteur were extremely wary of bulk data collection, and emphasised the difficulties in justifying wide-ranging intrusions into privacy. Like the European Courts, however, neither went so far as to suggest that it was inherently incapable of justification, given sufficient and effective safeguards.[105]

[105] Emmerson suggested that the justification would have to be "*compelling*": *ibid.*, para 9. Pillay sounded a similar note, arguing that stronger and more robust procedural safeguards are required to prevent arbitrary interference with the right to privacy: *The right to privacy in the digital age*, (June 2014), A/HRC/37, para 15. On the other hand, she did suggest that mandatory data retention "*appears neither necessary nor proportionate*": para 26.

6. POWERS AND SAFEGUARDS

6.1 It is illegal to intercept communications, or to obtain certain information about the use made of a telecommunications service, without the consent of the user.[1] However, Parliament has allowed a number of exceptions to this rule. This Chapter explains the current legal basis on which public authorities may collect and analyse people's communications, or records of their communications. Chapter 7 describes how the provisions set out below are implemented in practice.

Key concepts

6.2. The basic distinction that governs the operation of the law in this area is the difference between interception and communications data.

Interception

6.3. Interception is the collection of communications in the course of transmission.[2] RIPA provides that an interception takes place when "*contents of the communication* [are made] *available while being transmitted to a person other than the sender or intended recipient of the communication*"[3] The key word "*content*" is not defined in RIPA. Rather RIPA defines communications data, as set out below. Data that are not communications data are treated as content. Interception might consist of a wiretap on a telephone line or the gathering of emails or text messages in the course of transmission along communications cables. It makes available to the reader the contents of that communication and also the data relating to that communication (related communications data).[4]

6.4. RIPA s2(7) provides:

> "For the purposes of this section the times while a communication is being transmitted by means of a telecommunication system shall be taken to include any time when the system by means of which the communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it."

6.5. Therefore, perhaps surprisingly, an email is "*in the course of transmission*" when it is stored on a server. That view was affirmed by a recent decision of the Court of Appeal, which held that obtaining access to voicemails stored on a telephone is an interception.[5] As a result, certain techniques that provide access to the contents of stored communications, such as CNE or the hacking of cloud storage systems, may involve the interception of communications, which may be authorised by the various statutory powers set out below.[6]

---

1 RIPA ss1 (1) and (2); Wireless Telegraphy Act 2006 **[WTA 2006]** ss48 (1) and (4).
2 RIPA s1(1).
3 RIPA s2.
4 See the definition of related communications data in RIPA s20.
5 *R v Coulson and another* [2013] EWCA Crim. 1026.
6 By way of example, CNE or hacking might be authorised under ss5 or 7 ISA 1994.

Communications data

6.6. Communications data are data about use made of a telecommunications or postal service but not the contents of the communications themselves. Unlike intercepted material, communications data do not necessarily have to be collected when correspondence is "*in the course of its transmission*".[7] Communications data are generally obtained retrospectively from a service provider that retains that information (such as a mobile phone company), though when intercepted material is collected in the course of transmission, the related communications data are also collected. RIPA divides communications data into three categories:

(a) ***Traffic data*** which identifies the person, apparatus, location or address to or from which a communication is transmitted, and information about a computer file or program that has been accessed or run in the course of sending or receiving a communication.[8] Traffic data includes such matters as the geodata (or location data) produced by mobile phones on the move, as they communicate with base stations (cell-site data) and private WiFi networks, together with information on servers visited. The applicable Code of Practice states that website addresses or Uniform Resource Locators **[url]**s to the first slash e.g. https://www.google.co.uk are traffic data. On that basis the page address beyond the first slash, e.g. https://www.google.co.uk/#q=url+meaning, is content.[9] IP addresses are traffic data when they are allocated dynamically or temporarily to enable a communication to be routed.[10]

(b) ***Service use information*** relating to the use of a particular telecoms service. It is usually held by a service provider and records how many times and when a person made use of that service as well as which services they have used, such as amounts of data downloaded.[11] A simple example is an itemised phone bill.

(c) ***Subscriber information*** is all other information that the service provider holds about the person that uses the service. It covers the details that a customer provides to the service provider such as their address, telephone number or email address, but may include e.g. bank account data and personal information requested at sign-up.[12]

6.7. The three categories are assumed to be in descending order of intrusiveness, as may be seen from the (limited) respects in which the law treats them differently. Thus:

---

7 RIPA s1(1).

8 RIPA ss21(4)(a) and 21(6).

9 Acquisition Code, para 2.20: "*traffic data may identify a server or domain name (web site) but not a web page*." As pointed out by IOCCO there is a degree of ambiguity here, arising out of the absence of any definition of "*content*" within RIPA. IOCC Submission to the Review, paras 3.2.6 and 3.2.7.

10 *Ibid*. The Acquisition Code provides at 2.26 and fn 42 that dynamic IP addresses may be stored by a service provider in conjunction with subscriber information, in which case it would need to be treated as subscriber information, not traffic data.

11 RIPA ss21(4)(b) and 22(4).

12 RIPA s21(4)(c).

(a) Certain public authorities (including local authorities) are entitled only to request service use information and subscriber information.[13]

(b) Even bodies which are entitled to all three categories may be bound by different authorisation requirements: for example, a designated police inspector may request subscriber information, whereas a request for service use data and traffic data must be authorised by a superintendent.[14]

6.8. The categorisation has been criticised as obscure and unsatisfactory: I return to the point at 14.12 and Recommendation 12 below.

Powers outside RIPA

6.9. The current statutory framework governing investigatory powers has developed in a piecemeal fashion. The critical piece of legislation is RIPA. However, it is convenient first to introduce a number of other parallel statutes that authorise interception and the acquisition of communications data, but without (as a rule) the same degree of attention, analysis and oversight that is given to RIPA. RIPA itself makes clear that it does not supplant those other frameworks.[15] The Government expressed its intention some time ago to streamline the various statutory mechanisms via which data may be obtained.[16]

Non-RIPA interception

6.10. Apart from RIPA, WTA 2006 is the key statute allowing for the interception of communications.[17]

6.11. Sections 48 and 49 grant the Secretary of State and the Commissioners of Revenue and Customs a very broad power to authorise the interception of wireless or other communications. Interception must be necessary for a series of statutory purposes, including prevention of crime and disorder or the interests of national security. It must also be proportionate to the objective sought. The authority to intercept may be granted to any persons that the designated authority considers appropriate and for such time as the designated authority considers appropriate. The warrant must be issued by hand. The ISC reports that the Foreign Secretary has issued a single authorisation covering all of GCHQ's activities under the WTA 2006.[18]

6.12. The relationship between WTA 2006 and RIPA is somewhat opaque. There is no operational distinction between the two statutes. RIPA grants the power to interfere

---

13 The Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 480/2010).

14 *Ibid*. Schedule 1.

15 See for example s1(5)(c) which provides that interception in relation to stored communications has "*lawful authority*" if undertaken under "*any statutory power*." See also s80 which provides that nothing in RIPA should be construed as making it unlawful to engage in any conduct that "*would not be unlawful apart from this Act*."

16 *Home Office Review of Counter-Terrorism Powers,* (CM 8004) (January 2011), p. 29.

17 In addition, the interception of prisoners' communications takes place under a series of Prison Service Instructions (see s7 of the 2013 Annual Report of IOCCO). RIPA s4(4) provides that conduct that takes place in a prison is authorised by RIPA if it is conduct in exercise of any power conferred by or under any rules made under the Prison Act 1952 s47, the Prisons (Scotland) Act 1989 s39 or the Prison Act (Northern Ireland) 1953 (prison rules) s13.

18 ISC Privacy and Security Report, para 177.

with telecommunications systems, which are defined very broadly as a system "*for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy*."[19] WTA 2006 s48 may be used as a basis to authorise the use of wireless telegraphy apparatus to obtain information "*whether sent by means of wireless telegraphy or not*." In principle, at least, both RIPA and WTA 2006 might be used to intercept the same communications.

6.13. As to the exercise of those powers, WTA 2006 ss 49(2)(a) and (b) provide that it may not provide a basis for conduct that would be an offence under RIPA ss1(1) or (2), if engaged in without lawful authority. GCHQ considers this to be a reference to the definition of *"lawful authority*" in RIPA s1(5). Any interception under WTA 2006 is not lawful if it could also have been carried out under RIPA Part I Chapter 1.[20]

6.14. The position is clearer regarding the use of WTA 2006 to authorise access to communications data. WTA 2006 s49(2)(c) provides that an interception authority may not be given where it authorises conduct that could be authorised under RIPA Part I Chapter 2.[21]

6.15. A number of powers enable the contents of emails to be obtained when they are stored on a mobile phone or computer. In theory, they might be described as powers to "*intercept*" communications located on a server. However, it makes more sense to describe them as mechanisms by which lawful access may be granted to view "*stored communications*", as described in s1(5)(c) of RIPA:

(a) A judge may authorise a ***search order*** for private or commercial premises under the Police and Criminal Evidence Act 1984 [**PACE**] ss15 and 16 or the Supreme Courts Act 1981 s37. A search order will often include the right to access and remove files from the computers on site.

(b) Stored communications may also become available as a result of a ***production order*** requiring an individual to provide a phone, computer or certain physical files. The power to make production orders is set out in a number of different statutory provisions, many of which deal with specific types of crime such as drug trafficking or terrorism. PACE Schedule 1 also sets out a general power for the police to issue a production order where they suspect an indictable offence has been committed and a series of other conditions have been met.

(c) The ***Terrorism Act 2000*** provides an exception to the general requirement of judicial authorisation. Schedule 7 to that Act grants port officers (generally the police) a broad power to require persons passing through ports or airports to provide their property – including a telephone or laptop – without judicial authorisation. That property may be retained for up to a week, but information

19 RIPA s2(1).

20 One alternative reading would be that the WTA 2006 itself provides the "lawful authority" for conduct outside of RIPA and that it may be relied upon to intercept material that could also have been intercepted under RIPA.

21 Similar provision is made in the WTA 2006 s49(2)(d) with regard to conduct that is capable of authorisation under RIPA Part II.

downloaded is kept for much longer periods, pursuant to management of police information guidelines.[22]

Other non-RIPA powers

6.16. There are a number of other statutes that grant powers to public authorities and law enforcement agencies to interfere with telecommunications in some sense. One of the more important of those powers is set out in the Telecommunications Act 1984 **[TA 1984]** s94. Section 94 grants the Secretary of State a power to give "*directions of a general character*" to an individual, to the extent that they are "*necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom.*" The Secretary of State must consider that the content of the direction is proportionate to the objective sought.

6.17. The backdrop to s94 is the breakup of BT's monopoly of the telecoms market. The power to give directions was drafted into the Act that privatised the market. It is very broad in nature and imposes no limit the kinds of direction that may be given. There is nothing in the public domain concerning the use of that power and the exercise of the s94 power is not subject to any oversight or external supervision. In March 2015, the Interception of Communications Commissioner **[IOCC]** agreed formally to oversee directions under the TA 1984 s94, a task which he anticipated would require "*extra staff (and possibly technical facilities)*".[23]

6.18. A number of public authorities are also authorised to gather (or require the gathering of) data that may include communications data or communications data itself. A table of those public authorities has been provided to me by the Home Office and is located at Annex 6 to this Report. That list is not warranted to be comprehensive or up to date. But it is indicative, at least, of the wide range of powers available to a significant number of public authorities. It covers 46 different bodies that may require the production of data or communications data via 65 different statutory mechanisms. By way of example, the list identifies that the Department for Business Innovation and Skills may secure access to such data under:

(a) the Business Protection from Misleading Marketing Regulations 2008;

(b) the Companies Act 1985;

(c) the Consumer Credit Acts 1974 and 1985;

(d) the Consumer Protection Act 1987;

(e) consumer Protection from Unfair Trading Regulations 2008;

(f) the Copyright Design and Patents Act 1974 and 1988;

(g) the Enterprise Act 2002.

22 See D. Anderson, *The Terrorism Acts in 2013*, July 2014, Annex 2 and Annex 3.
23 *IOCC Report*, (March 2015), para 10.4.

6.19. I am informed that many, but not all, of those powers will be removed following the bringing into force of the Consumer Rights Act 2015.[24] The powers in (b) and some of those in (c) will remain on the statute book.

6.20. Three important general observations arise in connection with non-RIPA investigatory powers:

(a) There is little or nothing in the public domain that explains how frequently (if at all) they are used.

(b) It appears that at least some (perhaps many) Agencies and Departments exercise these powers without any published Code of Practice in place.

(c) As to the exercise of concurrent RIPA and non-RIPA powers, the position is a little clearer in respect of communications data than it is in relation to interception. The Acquisition Code states (at para 1.3) that public authorities should not use other statutory powers to obtain communications data from a postal or telecommunications operator unless that power explicitly provides that they may obtain communications data (or they are authorised to do so by a warrant or order from the Secretary of State or a person holding judicial office). DRIPA 2014 s1(6)(a) also states that a service provider must not disclose data retained under DRIPA 2014, except under RIPA Part I Chapter 2 or as provided by regulations.

6.21. I set out my recommendations concerning consolidation and reform in this area at 13.31-13.34 and Recommendations 1, 6 and 7 below.

Other intrusive capabilities

Surveillance, interference and CHIS

6.22. The security and intelligence agencies and police also have available to them a number of other intrusive capabilities such as intrusive and directed surveillance, interference with property, and CHIS. Those capabilities are provided for by RIPA Part II, Regulation of Investigatory Powers (Scotland) Act 2000 **[RIP(S)A]** and Police Act 1997 and are the subject of regular review by the ISCommr and OSC.

6.23. Those capabilities do not form part of the principal subject-matter of this Report, though a number of them are referred to for the purposes of comparison at 8.4-8.34 below.

CNE

6.24. But deserving of mention here is CNE (hacking, in common parlance), which may be carried out in order to access stored communications, amongst other things, under ISA 1994 ss5 and 7.[25]

---

[24] See in particular Schedule 6.

[25] See also 7.62-7.65 below. Accessing stored communications may be an interception, for the purposes of RIPA, as set out at 6.4-6.5 above.

6.25. ISA 1994 s5 gives the Secretary of State the power to issue warrants authorising MI5, MI6 and GCHQ to interfere with property in quite general terms. The interference must be proportionate to its objective and the material obtained must be used in carrying out those agencies' functions.[26] CNE was avowed for the first time by the Government, in February 2015, by the publication of the Draft Equipment Interference Code.[27] This makes clear that Equipment may include, but is not limited to, "*computers, servers, routers, laptops, mobile phones and other devices*."[28] It supplements the existing Covert Surveillance and Property Interference Code.

6.26. MI6 and GCHQ may both obtain authorisation, pursuant to ISA 1994 s5, to carry out equipment interference, such as hacking, in pursuit of their statutory functions, except where the property is in the British Islands and the purpose is the prevention or detection of serious crime. MI5 may also obtain s5 warrants in pursuit of its statutory functions, although where the function is to act in support of law enforcement and the property is in the British Islands, the warrant may only be authorised in order to secure the prevention or detection of what amounts to a serious crime.[29] MI5 may further undertake activity under ISA 1994 s5 in support of MI6 or GCHQ.

6.27. ISA 1994 s7 (which has been referred to as the "*James Bond clause*")[30] provides a power for the Foreign Secretary to authorise GCHQ or MI6 to carry out acts outside the British Islands that might otherwise be criminal offences or give rise to civil liability. GCHQ had five s7 class-based authorisations in 2014, removing liability for activities including those associated with certain types of intelligence gathering and interference with computers, mobile phones and other types of electronic equipment.[31] MI6 had eight class-based authorisations, removing liability for activities such as the identification and use of CHIS, directed surveillance and interference with and receipt of property and documents, and may seek further ministerial authorisations in respect of specific operations.[32]

6.28. The Draft Equipment Interference Code requires that an application should set out:

(a) the identity or identities, where known, of those who possess or use the equipment;

(b) sufficient information to identify the equipment;

---

26 ISA 1994 s5. The requirement that the Secretary of State consider the interference is proportionate and necessary was added by RIPA. MI6's functions include obtaining and providing information relating to the actions and intentions of persons outside the British Islands and to perform other tasks relating to the actions or intentions of such persons (ISA 1994, s1(1)). MI5's functions are to protect national security against espionage terrorism and sabotage from the actions of agents of foreign powers and also prevention of serious crime in the UK (Security Service Act 1989 **[SSA 1989]**, s1). GCHQ's functions are first to monitor or interfere with transmissions and to provide information about them and second to provide advice and assistance about languages and information security to the armed forces, the Government and other authorised organisations (ISA 1994, s3).

27 The Home Office have already published a Covert Surveillance and Property Interference Code of Practice **[Covert Surveillance and Property Interference Code]**.

28 fn 6, p. 5.

29 ISA 1994 s5(3B).

30 ISC Privacy and Security Report, para 236.

31 *Ibid.*, para 234.

32 *Ibid.*, para 233.

(c) the nature and extent of proposed interference;

(d) what the operation is expected to deliver;

(e) details of collateral intrusion;

(f) whether confidential or legally privileged material will be obtained;

(g) details of the offence or suspect offence;

(h) how the authorisation criteria are met;

(i) what measures will be put in place to ensure proportionality is maintained (e.g. filtering, disregarding personal information);

(j) where it is an urgent application, the supporting justification;

(k) any action which may be necessary to install, modify or remove software on the equipment; and

(l) in the case of renewal, the results obtained so far.[33]

6.29. The Secretary of State must be satisfied, before authorising the application, that it is necessary and proportionate, take into account whether the information could be obtained by other means and be satisfied that there are satisfactory arrangements in force in respect of disclosure of any information obtained.[34]

6.30. Once the information is obtained, there must be internal arrangements in force concerning the use of those data. The disclosure, copying and retention of those data must be limited to the minimum necessary for the discharge of the Services' functions. Those internal arrangements should be made available to the ISCommr. The material obtained, and all copies, should be destroyed as soon as they are no longer needed for the discharge of the Services' functions.[35]

6.31. The Draft Equipment Interference Code sets out substantial additional protections for legally privileged and confidential information. If the interference is intended to obtain such information, the application should say so expressly.[36] If it is likely that such material will be acquired, inadvertently, the application should identify the steps which will be taken to mitigate the risk of acquiring it and to ensure that any information acquired does not become used in law enforcement investigations or criminal prosecutions. Where acquisition of legally privileged material is likely or the intended result of the interference, the warrant will only be issued in "*exceptional and compelling circumstances*."[37]

33 Draft Equipment Interference Code, para 4.6.
34 *Ibid*., para 4.7.
35 *Ibid*., para 6.10.
36 *Ibid*., para 3.5
37 *Ibid*., paras 3.5-3.7.

6.32. The exercise of ISA 1994 ss5 and 7 powers is not subject to review by the IOCC but rather by the ISCommr, whose latest two annual reports set out the total number of warrants obtained by the security and intelligence agencies and the Ministry of Defence **[MoD]** (1,887 in 2013). It is not clear how many of those warrants were s5 warrants.

6.33. As to the relationship between CNE, carried out under ISA 1994 and interception under RIPA, the Draft Equipment Interference Code provides that if MI6 or GCHQ wishes to interfere with equipment that is overseas but the subject of the operation is known to be in the British Islands:

> "consideration should be given as to whether a section 8(1) interception warrant or a section 16(3) certification (in relation to one or more extant section 8(4) warrants) under the 2000 Act should be obtained."

It does not elaborate on what factors should be taken into account in the course of that "*consideration*."

RIPA powers

RIPA interception

6.34. The primary statute, pursuant to which telecommunications can be intercepted or communications data obtained, is RIPA. As set out above, RIPA sets out different mechanisms for the authorisation of interception and acquisition of communications data.

6.35. RIPA s71 requires the Secretary of State to publish guidance concerning the use and exercise of RIPA powers. Currently, this includes the Interception Code, the new Acquisition Code and the Retention of Communications Data Code of Practice **[Retention Code]**, laid before Parliament in March 2015.[38] Furthermore, the Home Office is consulting on a Draft Equipment Interference Code, which will regulate a specific area within the existing Covert Surveillance and Property Interference Code. The Home Office is also consulting on a Draft Interception Code.

6.36. The primary means by which an interception may be authorised under RIPA is via a warrant, issued under s5 and signed by a Secretary of State or Scottish Minister in person. The Secretary of State must believe that the warrant is necessary on grounds of national security, preventing or detecting serious crime, safeguarding the economic well-being of the UK or for the purpose of giving effect to an international agreement.[39]

6.37. The Secretary of State must also believe it is necessary and proportionate to the objective sought. That dual requirement of necessity and proportionality is a direct

---

38 As well as a Covert Surveillance and Covert Human Intelligence sources Code of Practice, not directly relevant to this Review.

39 RIPA s5(3).

import from the Article 8 case law of the ECtHR concerning the right to respect for private life.[40]

6.38. The power to apply for a warrant to intercept communications under RIPA is limited to the following organisations:

(a) MI5, MI6 and GCHQ;

(b) the NCA;

(c) the Metropolitan Police Service **[MPS]**, Police Service of Northern Ireland **[PSNI]** and Police Service of Scotland **[Police Scotland]**;

(d) HMRC; and

(e) the MoD.

6.39. Public authorities that are not authorised to obtain an interception warrant may ask the UK Central Authority, within the Home Office, to apply for a warrant on their behalf. The UK Central Authority then follows its normal procedures, as set out under RIPA. Interception can also happen at the request of an overseas legal authority through Mutual Legal Assistance Treaty **[MLAT]** arrangements. But this is an extremely rare occurrence. Such a request would be examined and authorised as if it were a domestic request.

6.40. With very few exceptions, material obtained under an interception warrant is not admissible as evidence in UK courts.[41] The Secretary of State may also impose restrictions on the use of material provided to overseas governments. I am informed by the Home Office that that is likely to include a request that the material is not used in evidence.

6.41. If one or both parties to a communication consent to its interception, a warrant is not needed. If only one party consents, approval is needed in line with the arrangements for a surveillance operation under RIPA Part II. Warrants are also not required for interception in prisons and for certain permitted business purposes, such as the prevention of fraud.[42]

Targeted warrants

6.42. RIPA s8 distinguishes between two different kinds of warrant that may be granted. Warrants issued under s8(1) are targeted, as they must describe either "*one person as the interception subject"* or "*a single set of premises*" where the interception is to take place under ss8(1) and (2). In practice, thematic warrants are sometimes issued under s8(1), which cover "*any organisation or any association or combination of*

40 For a fuller discussion see 5.18-5.24 below. As set out there, the interference must also be "*in accordance with the law*".

41 RIPA ss17-18; and see further at 9.16-9.18 below.

42 Prison Rules, National Security Framework, Function 4 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 s3.

persons." This interpretation of s8(1) was first avowed in the ISC Privacy and Security Report in March 2015.[43]

6.43. Section 8(1) warrants may authorise the interception of communications between two people in the British Islands, the communications of known individuals who are communicating outside the British Islands or between two persons overseas.

6.44. The Interception Code sets out the elements that a s8(1) warrant application must contain.[44] They include:

(a) the background to the operation in question;

(b) the person or premises to which the application relates (and how the person or premises feature in the operation);

(c) a description of the communications to be intercepted, details of the service provider(s) and an assessment of the feasibility of the interception operation where this is relevant;

(d) a description of the conduct to be authorised or the conduct (including the interception of other communications not specifically identified by the warrant as foreseen under RIPA s5(6)(a)) as it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data;

(e) an explanation of why the interception is considered to be necessary under the provisions of RIPA s5(3);

(f) a consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;

(g) a consideration of any unusual degree of collateral intrusion and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, or communications between a Member of Parliament and another person on constituency business, this must be specified in the application;

(h) where an application is urgent, supporting justification; and

(i) an assurance that all material intercepted will be handled in accordance with the safeguards required by RIPA s15.

Bulk warrants

6.45. Warrants issued under s8(4), often termed "*external*" warrants, authorise interception of communications where one or both of the senders or recipients of a communication

43 ISC Privacy and Security Report, paras 42-5.
44 Interception Code, para 4.2.

are located outside the British Islands.[45] Large volumes of data are carried around the world via fibre-optic cables and satellites. Section 8(4) warrants may be used to authorise the interception of all communications transmitted on a specified route or cable, or carried by a particular service provider.[46]

6.46. A s8(4) warrant application should specify:[47]

(a) the background to the operation in question;

(b) a description of the communications to be intercepted, details of the service providers and an assessment of the feasibility of the operation where this is relevant;

(c) a description of the conduct to be authorised which must be restricted to the interception of external communications, or to conduct necessary in order to intercept those external communications, where appropriate;

(d) the certificate that will regulate examination of the intercepted material;

(e) an explanation of why the interception is considered to be necessary for one of the RIPA s5(3) purposes;

(f) a consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;

(g) a consideration of any unusual degree of collateral intrusion, and why that intrusion is justified in the circumstances. In particular where the communication might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application;[48]

(h) where the application is urgent, supporting justification;

(i) an assurance that intercepted material will be read, looked at or listened to only so far as it is certified and it meets the conditions of RIPA ss16(2)-(6); and

(j) an assurance that the material intercepted will be handled in accordance with the safeguards required by RIPA ss15 and 16.

6.47. GCHQ currently only has the capacity to intercept the data travelling through a small percentage of the 100,000 bearers, including undersea cables, which make up the global communications core infrastructure.[49] Section 8(4) warrants play a strategic role in setting out which of these bearers are to be intercepted. They are issued by

45 RIPA s20.

46 See Charles Farr's witness statement of 2014 in the Liberty IPT Case **[Charles Farr Statement]**: https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/witness_st_of_charles_blandford_farr.pdf, para 139.

47 Interception Code, para 5.2.

48 The Draft Interception Code does not contain this requirement but does contain fuller provisions concerning the protection of confidential communications overall.

49 ISC Privacy and Security Report, para 27.

the Foreign Secretary to GCHQ and provide the legal basis for GCHQ's bulk interception capability.

6.48. Large volumes of material may be intercepted pursuant to a s8(4) warrant and thus become available for examination. At the same time as issuing a warrant, the Secretary of State must issue a certificate that describes the material that may be examined within that wider body of data. The certificates reflect the Priorities for Intelligence Collection **[PIC]** that are approved annually by the National Security Council after consideration by the Joint Intelligence Committee (the part of the Cabinet Office responsible for directing the security and intelligence agencies). The Secretary of State must be satisfied that it is necessary and proportionate to select and examine the data set out in the certificate.

6.49. As the ISC said of these certificates in its recent report:

> "We note that the categories are expressed in very general terms. For example: '*Material providing intelligence on terrorism (as defined by the Terrorism Act 2000 (as amended)), including, but not limited to, terrorist organisations, terrorists, active sympathisers, attack planning, fund-raising*.'"[50]

As a result, very large volumes of communications may be both intercepted and examined under a s8(4) warrant, though GCHQ's safeguarding and compliance mechanisms, and limitations on storage capacity, limit what can be actively processed or used.[51]

6.50. If an individual is known to be in the UK, and GCHQ wishes to select for examination his external communications, the Foreign Secretary may add his name to the certificate associated with the s8(4) warrant. In reality, most individuals in the UK who are of interest to the intelligence services are subject to a s8(1) warrant that will authorise the interception of both their internal and external communications.[52]

6.51. In summary, the boundary between targeted and bulk warrants is comparatively clear. A targeted warrant must be directed at a person (or association of persons) or premises and it must include schedules setting out the factors to be used to identify the communications to be intercepted. A bulk warrant must be targeted against external communications and is not required to include schedules that identify the communications to be sought. However, it must be accompanied by a certificate from the Secretary of State issued in accordance with ss8(4) and 16(3).

6.52. The boundary between "*internal*" and "*external*" communications is less straightforward. OSCT's interpretation was, as set out in the Charles Farr Statement, that:

---

50 ISC Privacy and Security Report, para 101.

51 For a fuller discussion of some of the process adopted by GCHQ in respect of data analysis see: *IOCC Report,* (March 2015) para 6.37-40.

52 Though individuals targeted under a s8(1) warrant may also be subject to additional coverage of their external communications under a s8(4) warrant.

(a) Two people in the UK who email each other are engaging in internal communication, even if they use an email service which is housed on a server in the United States. The fact that the communication travels via a server overseas does not make it external, but it may well be collected under a warrant targeting external communications.[53]

(b) A person in the UK who communicates with a search engine overseas is communicating with a server overseas and engaging in an external communication. Likewise a person who posts a public message such as a tweet or Facebook status update, is sending an external communication unless all the recipients of that message are within the British Isles.[54]

This was not clear prior to the publication of Mr Farr's statement. Some have considered those distinctions counter-intuitive: for example, many people might not consider a Google search to be a communication at all, let alone an external communication.

6.53. Further potential confusion follows from the fact that internal communications are collected under external warrants. RIPA s5(6) allows the collection of information that is not specified in the warrant, if it is necessary in order to collect the information that is specified in the warrant.[55] As explained in the Charles Farr Statement, it is inevitable that there is "*by-catch*" of internal communications because s8(4) bulk interception takes place at the level of communications cables.[56] It is generally accepted that the collection of such material cannot be avoided.

6.54. As the IPT noted, in a recent judgment concerning the s8(4) framework, in practical terms it is s16 of RIPA that must do the "*heavy lifting"* when it comes to the distinction between internal and external communications.[57]

6.55. Section 16 sets out the extra safeguards in respect of material intercepted pursuant to a s8(4) warrant. In order to be examined, material must fall within the Secretary of State's certificate and it must not be selected according to a factor that is "*referable to an individual who is known for the time being to be in the British Islands"* and the purpose of which is to identify his communications (s16(2)).

6.56. However, ss16(3)-(5) provide for two exceptions to that position:

(a) The external communications of a person known to be in the British Islands may be selected for examination if the Secretary of State certifies that that is necessary for the purposes of national security, the prevention or detection of serious crime or protecting the economic wellbeing of the UK: s16(3). In practice the Foreign Secretary approves one or more lists of such targets every six months, though he can add names at any time. Most UK-based individuals who are subjects of interest to the security and intelligence agencies or law

53 Interception Code, para 5.1; Charles Farr Statement, para 128.
54 Charles Farr Statement, paras 134-137.
55 The same provision also applies to internal warrants. "*Collateral"* material may be gathered where it is technically necessary in order to carry out the s8(1) warrant.
56 Para 139.
57 Liberty IPT Case, judgment of 5 December 2014, para 101.

enforcement are however targets of s8(1) warrants issued by the relevant Secretary of State, which will authorise the interception of all their communications, where necessary with the assistance of GCHQ.

(b) If the person to whom the warrant is addressed concludes that there has been a relevant change of circumstances, in essence that the individual has now entered the British Islands, the material may still be selected for a brief period of time. The short window of five days that is allowed for the selection of material under RIPA s16 provides the opportunity to obtain a certificate from the Secretary of State that the examination of that material is necessary (ss16(4)-(6)) or to obtain a s8(1) warrant to intercept all of their communications.

6.57. The practical consequence of this is that:

(a) Some internal communications are unavoidably intercepted under warrants for the interception of external communications.

(b) Material intercepted under external warrants is subjected to computer-based selection (for example by reference to simple selectors such as email addresses or telephone numbers, or using complex selectors based on a combination of factors) in order to find items of intelligence interest. Items may not be selected for reading by reference to an individual known to be in the British Islands, where the purpose is the identification of that person's communications.

(c) However internal communications may be read if:

- they are selected to be examined by reference to another factor (although GCHQ inform me that they may not use this route in order to deliberately seek access to internal communications and that it is unlikely to occur in practice); or

- the Secretary of State certifies that it is necessary to select and examine a person's communications (pursuant to s16(3)) and those communications include some internal communications.[58]

(d) Where the original intention is to obtain internal communications, a s8(1) warrant will be sought.

6.58. Furthermore, there are no restrictions on the examination of communications data relating to internal communications that are incidentally collected under a s8(4) warrant. That material may be examined, if it can be shown to be necessary and proportionate to the purposes of the examining authority.

6.59. The proportionality of the mechanisms employed pursuant to s8(4), and the sufficiency of the safeguards set out in s16, are currently the subject of a challenge before the

[58] As noted by the ISC Privacy and Security Report, paras 113-115, GCHQ does not always apply for s8(1) warrants in relation to the communications of individuals in the UK, although GCHQ considers that the process for modifying s16 certificates provides equivalent safeguards. The ISC noted that the modification process does not require consideration of all of the elements that are necessary before a s8(1) warrant is sought.

IPT. The Tribunal has already held that the s8(4) framework is "*in accordance with the law*," in the sense that it the manner in which it operates is sufficiently foreseeable.[59] However, the Tribunal is yet to rule on the proportionality of the methods deployed to carry out bulk interception under s8(4).

RIPA access to communications data retained by service providers

6.60. Communications data are collected and held by service providers. They already hold data on their customers (subscriber information) and will generate service use information and traffic data depending on their business model. That information is necessary in order to enable communications to be routed successfully and also for billing and marketing purposes. RIPA Part I Chapter 2 sets out the framework under which public authorities may seek access to the data held by the service providers.

6.61. Service providers may be required to retain data for up to a year on receipt of a notice from the Home Secretary, issued under DRIPA 2014 s1. The Retention Code provides at para 3.3 that companies with larger customer bases are more likely to receive a notice. Other service providers are not compelled to retain data, but all service providers are obliged to hand over data to a public authority when they receive a request.[60] Those data which might be required to be retained are set out in the Schedule to the Data Retention Regulations.[61] Companies that have received a notice may be asked to retain data including:

(a) the sender or recipient of a communication (whether or not a person);

(b) the time or duration of a communication;

(c) the type, method, pattern or fact of a communication;

(d) the telecommunications system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted; and

(e) the location of any such system.[62]

6.62. A voluntary code of practice, drawn up under the Anti-Terrorism Crime and Security Act 2001 **[ATCSA 2001]**, permits service providers to retain other data not required under DRIPA 2014, such as phone cell data and the times at which emails are sent and received.[63]

6.63. CTSA 2015 provided for the first time that service providers should generate and retain data that they did not need for their own business purposes. Section 21 provides that service providers may be required to retain data necessary to resolve IP addresses to an individual or device. In brief, that information enables public authorities authorised to acquire communications data to confirm which device was accessing particular

59 Liberty IPT Case, judgment of 5 December 2014.
60 RIPA s22(3A).
61 SI 2042/2014.
62 Retention Code, para 2.14.
63 Retention of Communications Data under Part 11: Anti-Terrorism, Crime & Security Act 2001: Voluntary Code of Practice.

services at a particular point in time, though IP address resolution is still not possible in all cases.

6.64. RIPA Part I Chapter 2 sets out the basis on which public authorities may seek and obtain access to communications data. There are four major differences between the law as it relates to interception and to communications data:

(a) The ***list of public authorities*** which can obtain communications data is much longer: a total of about 600 organisations as opposed to nine.

(b) The ***list of grounds*** that can be used to justify access to communications data is longer. As well as national security, detecting crime or disorder and the economic well-being of the UK, communications data can be accessed on the grounds of public safety, public health, collecting taxes or preventing death or injury in an emergency. As with interception, those grounds are subjected to a proportionality assessment.[64]

(c) The ***content of the notice or authorisation*** does not need to be tightly defined or restricted to an individual. It only needs to describe the communications data that are required.[65] For example, an authorisation might describe the IP addresses of all users who have accessed a particular website or the phone numbers of everyone who has telephoned a particular number.

(d) The ***power to authorise*** interception lies with the Secretary of State, whereas authority to obtain communications data resides with a designated person **[DP]** at middle management level: for example a superintendent or inspector in the police, or a Grade 7 in certain parts of the Civil Service.[66]

6.65. But that is not to say that the process is one of simple self-authorisation. Generally speaking, the DPs (as prescribed by an order of the Secretary of State) work in conjunction with a Single Point of Contact **[SPoC]**. SPoCs fulfil two principal roles:

(a) advising whether an application is appropriate, lawful and practical, and

(b) providing a consistent and knowledgeable interface with the service providers.

6.66. The role of SPoCs is not set out in statute, but in the Acquisition Code.[67] It is the responsibility of the DP, rather than the SPoC, to give approval to a request to obtain access to communications data. The DP must usually be independent of the investigation concerned and of the SPoC.

6.67. Local authorities are in a somewhat different position. As a result of changes made by the Protection of Freedoms Act 2012 **[PFA 2012]**, local authorities are required to apply to the magistrates' court for that authorisation or requirement, which may then

64 RIPA s22(2).
65 RIPA s23(2)(b).
66 See RIPA s25(2). For a full list see Regulation of Investigatory Powers (Communications Data) Order 2010, Schedules 1 and 2.
67 Paras 3.19-3.30.

be forwarded to the service provider.[68] The application must now be made first to the National Anti-Fraud Network **[NAFN]**, a kind of external SPoC, which then forwards it to the magistrates' court. More detail is at 7.60 below.

6.68. The applicant applying for access to communications data must, in writing:[69]

(a) provide the name or designation and the office, rank or position held by the person making the application;

(b) include a unique reference number;

(c) include the operation name (if applicable) to which the application relates;

(d) specify the purpose for which the data is required, by reference to a statutory purpose under s22(2) of RIPA;

(e) describe the communications data required, specifying where relevant, any historic or future date(s) and where appropriate time period(s);

(f) describe whether the communications data relate to a victim, a complainant, a suspect, a next of kin, vulnerable person or other person relevant to the investigation or operation;

(g) explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it; and

(h) consider, and where appropriate describe, any likely collateral intrusion (the extent to which the privacy of any individual not under investigation may be infringed), and why that intrusion is justified in the circumstances;

(i) consider, and where appropriate describe, any possible unintended consequences of the application; and

(j) identify and explain the time scale within which the data is required.

6.69. Where approval is given orally in cases of urgency, retrospective written notification should be given within one working day.[70]

6.70. In each organisation the process of communications data acquisition and disclosure is overseen by a Senior Responsible Officer responsible for the oversight and integrity of the arrangements for acquiring and using communications data within their organisation.[71]

---

68 See RIPA s23A.
69 Acquisition Code, para 3.5.
70 *Ibid.*, para 3.69.
71 *Ibid.*, para 3.31.

RIPA safeguards

6.71. RIPA sets up a range of safeguards to ensure the proper collection, storage and use of intercepted communications and communications data. Those safeguards do not apply to the collection of information via the other routes identified above, which may be governed by their own safeguards such as the handling arrangements under the SSA 1989 and ISA 1994.

6.72. RIPA s15 contains a set of general safeguards concerning intercepted material:

(a) The number of persons, copies and times that that information is shared is restricted to the minimum that is necessary (s15(2)). The Interception Code makes clear that this applies to persons both within and outside the agency.[72] As a result, data are only shared only on a "*need-to-know*" basis. Further disclosure requires either the originator's permission or the application of explicit safeguards to the secondary recipients. Those safeguards are not in the public domain.[73]

(b) Material must be destroyed as soon as there are no longer any grounds for retaining it for an authorised purpose (s15(3)).

(c) The material must be stored in a secure manner (s15(5)).

6.73. Unlike the position in relation to intercepted material, RIPA places no restrictions on the retention or use of communications data.[74] Section 23(3) provides that a s24(4) notice to a service provider may require it to disclose data to another police force. However, further disclosure between authorities is not specifically addressed either within RIPA or the Codes of Practice.

6.74. Therefore, the framework that largely or exclusively controls its use is the Data Protection Act **[DPA 1998]**.[75] But DPA 1998 s28 allows the Secretary of State to issue a certificate excluding material from the scope of the data protection principles and from parts of the Act on national security grounds.[76] I was informed by GCHQ that such certificates are sometimes issued by the Secretary of State but that they only exempt the personal data held by it from the obligation to comply with the first, second and eighth (as well as part of the sixth) data protection principles.[77]

---

72 Interception Code, para 6.4.

73 *Ibid.*, para 6.5.

74 Unless that communications data is related communications data collected in association with an interception warrant. The Interception Code contains surprisingly little detail on the use such material.

75 The Criminal Procedure and Investigations Act 1974 and the Management of Police Information principles will also apply in the context of material obtained for the purposes of a criminal investigation.

76 Acquisition Code, chapter 7, addresses data use to some degree, though it is focused on the conduct of service providers, rather than the authority that has gathered the data.

77 Those certificates are not drafted to as to exempt the intelligence agencies from compliance with the fifth and seventh principles and as a result data must not be kept for longer than is necessary, having regard to the purposes for which it was obtained. Furthermore those data must be subject to appropriate technical and organisational measures against unauthorised or unlawful processing of the data and accidental loss of the data in question.

6.75. Related communications data obtained pursuant to an interception warrant are treated in the same way as intercepted material. The s15 principles, set out above, apply to that material.

6.76. But RIPA s16 only applies to intercepted material and not to related communications data, which may be selected and reviewed according to a factor which is referable to an individual who is known for the time being to be in the British Islands.

Safeguards for confidential material

6.77. RIPA itself offers no guidance concerning the treatment and handling of confidential communications, such as those covered by LPP. The Interception Code offers some guidance on those questions. It states that, where it is likely that privileged communications will be intercepted, that should be stated on the face of the warrant application and weighed by the Secretary of State when determining whether or not to grant it. The Interception Code also states that caseworkers should be "*alert to any intercept[ed] material which may be subject to legal privilege*."[78] It does not state what steps should be taken if legally privileged material is identified. Similar guidance is given concerning the treatment of confidential personal information and journalistic material.[79]

6.78. The IPT declared in February 2015 that the UK Government's regime for the interception, analysis, use, disclosure and destruction of legally privileged communications contravened ECHR Article 8 between 2010 and early 2015.[80] That declaration was made following an admission by the Government to that effect. The new Acquisition Code and Draft Interception Code were published shortly afterwards.

6.79. The new Draft Interception Code expands on the protections afforded to confidential communications in the Interception Code. Where the interception is intended to intercept legally privileged communications, the Secretary of State must be satisfied that there are "*exceptional and compelling circumstances that make the warrant necessary*."[81] Where such communications will be intercepted, although that is not the intention, the application for a warrant should identify the steps which will be taken to mitigate the risk of obtaining legally privileged information.[82] Officials who examine intercepted communications should seek advice where there is any doubt concerning the privileged nature of the communication and any legally privileged material that is retained or disseminated must be accompanied by a clear warning that it is subject to legal privilege.[83] The Draft Interception Code sets out similar provisions in respect of journalistic or other confidential material but the threshold for access is not as high as that in respect of legal privilege.[84]

78 Interception Code, paras 3.2-3.8
79 *Ibid*,. paras 3.9-3.11.
80 In the Belhadj IPT Case, the order in relation to which can be found at: https://www.judiciary.gov.uk/wp-content/uploads/2015/02/belhadj-order-open-.pdf.
81 Draft Interception Code para 4.8.
82 *Ibid*., para 4.7
83 *Ibid.*, paras 4.12-4.14
84 *Ibid*., paras 4.19-4.25.

6.80. RIPA is silent in relation to communications data that may attract privilege. The Acquisition Code states that communications data are not subject to professional privilege but also that it may be possible to "*infer an issue of sensitivity from the fact that someone has regular contact with, for example, a lawyer or journalist*."[85] In such circumstances, "*special consideration"* should be given to necessity and proportionality.[86] In cases where an application is made for communications data in order to identify a journalist's source, judicial authorisation must be obtained via the procedures in PACE.[87] In practice, it appears that the new Acquisition Code recognises that communications data may attract professional privilege and require special treatment on account of its confidential nature.

Data Sharing

Within the UK

6.81. RIPA s15 requires that disclosure of intercepted material is restricted to the minimum necessary for the authorised purposes set out in s15(4).

6.82. Material obtained pursuant to a s8(4) warrant may only be read, looked at or listened to by any person if it is certified for examination by the Secretary of State (see the discussion of RIPA s16 at 6.54-6.59 above).

6.83. The position in respect of communications data that have been acquired under RIPA is more complex. As explained at 6.71 above, material obtained on national security grounds may only be subject to certain aspects of DPA 1998. In any event, it should not be retained for longer than necessary, having regard to the purposes for which it was obtained. That principle will also apply to those with whom the data is shared.

6.84. There is no restriction equivalent to RIPA s15 on the sharing of raw communications data within government: but I was told that it is not a common practice. Communications data, as well as interception product, will typically inform reports from the security and intelligence agencies. This analysed intelligence is circulated to Ministers, officials and others with the appropriate security clearance, who have a need to receive the information. Circulation of intelligence product is tightly controlled by the security and intelligence agencies, not just to meet the legal requirements of minimising intrusion but also to ensure that their sources and methods are given the least exposure.

Data from the UK

6.85. I am informed by GCHQ that RIPA ss15(6) and (7) set out the restrictions on sharing intercepted material with other states in circumstances where such exchange is requested under a mechanism such as MLAT. In essence, the Secretary of State must be satisfied that the receiving state will apply minimisation techniques "*to such extent (if any) as the Secretary of State thinks fit"* (s15(7)(a)).

---

85 Acquisition Code, paras 3.72-3.
86 *Ibid*., para 3.74.
87 *Ibid*., para 3.78.

6.86. I am informed that SSA 1989 s2(2) and ISA 1994 s4(2) are considered before any RIPA safeguards are engaged. In brief, information must not be shared unless that sharing is necessary for the purpose of the proper discharge of the security and intelligence agencies' functions.

6.87. As to RIPA itself, information sharing (outside of MLAT) is governed by ss15(1)-(3), which set out the general safeguards on information use (as described above). In brief, the Secretary of State must be satisfied that the number of persons to whom the data is disclosed and number of copies made are limited to the minimum that is necessary and the material is destroyed as long as there are no longer any grounds for retaining it. As a result, in practical terms, the safeguards applying to the use of such data are entirely subject to the discretion of the Secretary of State. There are no further safeguards set out in the Interception Code.

6.88. RIPA itself imposes no limits on the sharing of communications data obtained from service providers under RIPA Part II Chapter 1 with overseas governments.[88] However, the Acquisition Code does provide some further information in respect of specific requests for information:

(a) Communications data may be sought via an MLAT mechanism, whereby an overseas court or prosecuting authority formally requests material stored in the UK.[89] This is considered by the UK central authority in the Home Office and, if accepted, passed to the appropriate public authority to action in line with the Acquisition Code.

(b) Overseas authorities may also make non-judicial requests for assistance to public authorities in the UK. The UK authority must consider the necessity and proportionality of each case and may then obtain that data via its powers under RIPA. Before it acquires and transfers that data, the UK authority must consider whether the data will be adequately protected outside the UK and may attach conditions to the processing storage and destruction of the data.[90]

(c) If the requesting state is within the EU, communications data can be disclosed without consideration of further safeguards. The European Commission has also determined that certain countries (such as Canada and Switzerland) have adequate safeguards in place. In all other circumstances, the public authority must consider whether the data will be adequately protected.[91]

(d) However, the Code recognises that "*there may be circumstances when it is necessary, for example in the interests of national security, for communications data to be disclosed to a third party country, even though that country does not have adequate safeguards in place to protect the data.*"[92]

88 Communications Data associated with intercepted material is governed by ss15(1)-(3).
89 Acquisition Code, paras 7.13-14.
90 *Ibid*., paras 7.15-17.
91 *Ibid*., paras 7.18-20.
92 *Ibid*., para 7.21.

Data to the UK

6.89. Prior to the recent Liberty IPT Case, there was limited concrete information in the public domain concerning the safeguards that were applied to the receipt, in the UK, of data from overseas governments. Neither RIPA nor the Codes of Practice deal with this question at all. There are general constraints on the actions of the security and intelligence agencies. As MI5 argued before the IPT, it is only entitled to obtain information "*so far as necessary for the proper discharge of its functions.*"[93] Other similar constraints arise out of ISA 1994 ss1-4, DPA 1998 s4, HRA 1998 s6 and the Counter-Terrorism Act 2008 s19.[94]

6.90. The ISC reported in 2013 that "*in each case where GCHQ sought information from the US, a warrant for interception, signed by a Minister, was already in place, in accordance with the legal safeguards contained in [RIPA]*".[95] In the course of the Liberty IPT Case, the security and intelligence agencies disclosed that data might, at least in theory, be obtained in another scenario. Data may either be sought from overseas governments when:

(a) an interception warrant had been granted authorising the interception of those communications but they could not be obtained under that warrant and it would be necessary and proportionate to obtain those communications;[96] or

(b) making the request does not "*amount to a deliberate circumvention of RIPA*". For example, in circumstances where it is not technically feasible to obtain that material under RIPA, and it is necessary and proportionate to gain access to it. A request of that kind should be personally considered by the Secretary of State.[97] The security and intelligence agencies confirmed that this would only take place "*in exceptional circumstances, and has not occurred as at the date of this statement"*.[98]

6.91. The IPT concluded that, prior to that disclosure, the regime that governed the receipt of private communications from the US Government (obtained by the US Government via UPSTREAM and PRISM) had not been "*in accordance with the law"*.[99] That framework had not been sufficiently foreseeable and had not satisfied the standard required by the Article 8(2) case law in the national security context.[100] However, the IPT also held that, following the disclosures made in the course of the hearing, the security and intelligence agencies had placed the current arrangements on a sufficiently clear footing and the requirements of Articles 8 and 10 were now satisfied. That latter conclusion is subject to challenge in the ECtHR.

---

93 SSA 1989 s2(2)(a).

94 Liberty IPT Case, judgment of 5 December 2014, paras 18-19.

95 *Statement on GCHQ's alleged interception under PRISM*, (July 2013), para 5.

96 Such a warrant being either: i) a s8(1) warrant; ii) a s8(4) warrant and a certificate and a s16(3) modification (for those within the British Islands); or iii) a s8(4) warrant with a certificate.

97 Liberty IPT Case, judgment of 5 December 2014, para 47.

98 *Ibid*., para 48(1).

99 Liberty IPT Case, judgment of 6 February 2015, para 23.

100 I address this decision and the principles governing this area of law in more detail at 5.19-5.20 and 5.35 above.

6.92. The IPT also considered the use and safeguards applying to data, once it had been received from overseas. The security and intelligence agencies disclosed that information that is covered by a warrant, but cannot be obtained by the UK Government, are "*subject to the same internal rules and safeguards as the same categories of content or data, when they are obtained directly by the Intelligence Services as a result of interception under RIPA"*.[101]

6.93. However, the IPT expressed its concern that the same principle would not apply to information requested on the second ground: data that it was not feasible to collect under RIPA. As the Tribunal noted, s16 would not (automatically) apply in those cases. In its December judgement, the IPT directed that "*there ought to be introduced a procedure"* addressing this issue.[102] The Tribunal's judgment in February stated that equivalent safeguards are now in place for material that may be obtained via that second route.[103]

6.94. The Tribunal also considered the nature and operation of confidential procedures governing the use of data "*below the waterline*" that it considered were adequately "*signposted*" by the disclosures and by other material already in the public domain.[104] The Claimants argued that that practice was improper[105] but the IPT disagreed, and the issue is now before the ECtHR.

Extra-territorial reach of RIPA

6.95. It is increasingly common that content and communications data are located outside the UK but not in the possession of a foreign state or its security and intelligence agencies. Most commonly that material is in the possession of overseas service providers, presenting unique jurisdictional challenges when UK law enforcement agencies wish to gain access to those data. DRIPA 2014 s4 seeks to address that problem by spelling out the extraterritorial effect of RIPA ss11, 12 and 22.[106]

6.96. In respect of interception warrants, under RIPA s11(4), any person is obliged to take steps to give effect to a warrant served on them "*whether or not the person is in the United Kingdom"*. That person is not required to take steps which "*it is not reasonably practicable for him to take"*, and consideration will be given to the requirements or restrictions under the law of the country or territory in which he resides (s11(5A)). However, if a person "*knowingly fails to comply"* with these duties, they may be guilty of an offence (s11(7)). Enforcement, including persons outside of the UK, may be effected through the civil courts.

6.97. RIPA s12 is also amended by DRIPA 2014 so that the Secretary of State can by order impose an obligation on a person, whether or not that person is within the UK, who is providing public postal services or public telecommunications services to secure that

101 Liberty IPT Case, judgment of 5 December 2014, para 47.
102 *Ibid.*, para 53.
103 Liberty IPT Case, judgment of 6 February 2015, paras 24-32.
104 Liberty IPT Case, judgment of 5 December 2014, para 50(i).
105 *Ibid.*, para 49(i).
106 The Government's position, which not everyone accepts, is that the relevant sections of RIPA already had extraterritorial effect.

requirements to provide assistance in relation to interception warrants are complied with.

6.98. For communications data, RIPA ss22(5A)-(5B) state that an authorisation or a requirement in accordance with a notice may relate to conduct outside the UK and may be given to a person outside the UK. Under s22(6), it shall be the duty of the service provider "*whether or not the operator is in the United Kingdom"* to comply with the requirements of any notice given to him under s4, so long as "*reasonably practicable"* (s22(7)), although unlike interception there is no requirement to consider the restrictions of the law of the territory in which that person operates. The duty can be imposed, including on those outside the UK, by civil proceedings for an injunction or for specific performance of a statutory duty (s22(8)). In practical terms, the UK Government has asserted its right to order overseas service providers to provide communications data when a notice is served on them.

6.99. Whether or not the UK Government could enforce these obligations in relation to service providers has not yet been tested and there remain some overseas service providers who do not consider they are bound by RIPA. As a matter of practice, such cooperation as is forthcoming from overseas CSPs comes from informal requests for assistance.

Oversight

The IOCC

6.100. The office of IOCC is constituted under RIPA to keep under review the exercise and performance by the Secretary of State and other public authorities of their functions under RIPA Part I.[107] The IOCC must hold, or have held, high judicial office. The current Commissioner is Sir Anthony May, a former judge of the Court of Appeal. He reports to the Prime Minister, who lays that report before Parliament, every six months.[108]

6.101. The IOCC holds the public authorities that exercise RIPA powers to account, and seeks to improve compliance (and public confidence) by means of scrutiny. He selects and reviews a sample of warrants, and assesses their necessity and proportionality.[109] He also reviews errors that have been identified by public authorities, identifies further errors and assesses any mitigating steps that have been put in place. He cannot disclose the details of any individual warrant or communications data acquisition but a part of his role is to examine how RIPA powers are being used, whether they are being abused and if so to draw the fact to public attention in his six-monthly reports to the Prime Minister (which are laid before Parliament).

---

107 RIPA s57. Other commissioners include the ISCommr, who has an equivalent role, and the Surveillance Commissioner: see 6.22 above.

108 RIPA s58(4).

109 For a discussion of the IOCC's query based sampling method see *IOCC Report*, (March 2015), paras 6.54-6.59.

6.102. IOCCO has in recent years under successive Commissioners and the Head of IOCCO, Joanna Cavan, built up formidable expertise in the nuts and bolts of interception, to add to its longer experience of communications data. By way of illustration:

(a) IOCCO employs nine experienced and technically skilled inspectors, many with a police or intelligence background, who were given access without reservation not only to all the material they requested but to the Agencies' own systems and to the processes of the warrant granting department **[WGD]** that assists each relevant Secretary of State. Similar access is also granted to each public authority that is entitled to acquire communications data under RIPA Part I Chapter 2.

(b) The Commissioner's latest report sets out the manner in which IOCCO inspected every aspect of the interception process, from compliance with the Interception Code and the previous Communications Data Code to the actual application of individual selection criteria, the retention, storage and destruction of intercepted material, security and administrative safeguards and audit checks carried out by the Agencies.[110]

(c) These inspections are by no means whitewashing exercises. Three significant caveats were set out in the published report concerning the period up to the end of 2014 and subsequently investigated;[111] more than 400 recommendations were made to public authorities; the necessity and proportionality of some interceptions was challenged and a total of 69 recommendations were made to the nine interception agencies in relation to pre-authorisation or authentication processes, the enhancement of retrospective audits and a more explicit role for the Commissioner in the audit process.[112]

6.103. There are constraints (not least in RIPA itself) on the transparency that is possible in this area. It is also unfortunate that the IOCC's reports do not receive more widespread publicity, whether because of their technical nature or the sense that the Commissioner and his staff are more interested in doing an excellent job than in gaining publicity for it.[113] But having spoken in depth to IOCCO, and reviewed a number of reports of similar review bodies from different countries, I would comment that they are a model of their kind.

6.104. As set out above, in March 2015, the IOCC agreed formally to oversee directions under TA 1984 s94, a task which he anticipated would require "*extra staff (and possibly technical facilities)*".[114] The ISCommr oversees the exercise by the Agencies of their ISA 1994 and SSA 1989 powers, as set out above. However, there is no entity appointed to oversee access to communications data under any of the myriad routes

110 *IOCC Report*, (March 2015), chapter 6.
111 *Ibid.,* para 6.35.
112 *Ibid.,* paras 1.9, 6.39-6.40, 6.69-6.70.
113 Though IOCCO has a twitter feed (@iocco_oversight), on which it has shown itself willing to engage informally with critics and sceptics; and an impressive list of public engagements is given in its March 2015 report at para 3.4.
114 *IOCC Report*, (March 2015), para 10.4.

set out in Annex 6 to this Report, and IOCCO cannot and does not review that process. As a result, there is far less transparency concerning those processes.

The Investigatory Powers Tribunal

6.105. The IPT hears complaints about conduct in connection with the interception of communications and gathering of communications data (by all authorities, not just the security and intelligence agencies).[115] It also has jurisdiction to determine complaints under HRA 1998 s7 in respect of the actions of the security and intelligence agencies.[116] The IPT is established under RIPA, but its role and remit goes beyond it.

6.106. For some years after its establishment in October 2000, and despite its distinguished membership, the IPT was a little-known body. Its rules prohibited the holding of public hearings, and public judgments were rare. Its profile as a robust scrutiny mechanism was not assisted by the fact that out of the 1,673 complaints determined by the end of 2013, only 10 were upheld – five of them involving members of the same family, and none of them against the security and intelligence agencies.[117] This is not a criticism of the IPT, whose members are drawn from the upper reaches of the judiciary and legal profession. But coupled with the opaque procedures provided for in the IPT's rules, it did not promote public confidence in, or even knowledge of, the institution.

6.107. The IPT's journey out of the shadows began in January 2003, when it authorised its first open hearing (in a complaint concerning a possible RIPA Article 8(1) warrant), notwithstanding the rule that its proceedings had to be conducted in private.[118] Other rules (concerning restrictions on disclosure and evidence, secrecy of proceedings and the non-provision of reasons to unsuccessful complainants) continued to be contested as contrary to the principle of equality of arms, guaranteed by Article 6 of the ECHR. But in its *Kennedy* judgment of May 2010, the ECtHR concluded that the procedures of the IPT did not violate Article 6. It emphasised, in doing so:

> "the breadth of access to the IPT enjoyed by those complaining about interception within the United Kingdom and the absence of any evidential burden to be overcome in order to lodge an application with the IPT."[119]

The European Court thereby accepted that once general legal issues have been determined in public, any consideration of the specific facts of the case will take place in private and without the participation of the complainant.[120]

6.108. Even prior to the Snowden revelations, the IPT had in *British Irish Rights Watch* ruled in an open judgment that the provisions for intercepting and accessing material

115 RIPA s65(5).
116 RIPA s65(2)(a).
117 Interception of Communications Commissioner Annual Report 2013; subsequent figures on IPT website. According to the IPT's website, around half of the complaints received in recent years have been adjudged "*frivolous or vexatious*" under RIPA s67(4): http://www.ipt-uk.com/section.aspx?pageid=5.
118 IPT/01/62 and IPT/01/77 *Kennedy*, ruling of 23 January 2003. The hearing, on issues of legal principle, was held in July 2004: IPT/01/62, ruling of 9 December 2004.
119 Application no. 26839/05 *Kennedy v United Kingdom*, Judgment of 18 May 2010, para 190.
120 *Ibid.*, para 98.

covered by a RIPA s8(4) warrant were sufficiently accessible and foreseeable to be in accordance with the law.[121]

6.109. After 2013, a number of NGOs and individual brought claims to the IPT seeking detailed consideration of the legality of elements of the investigatory powers regime. There were several open hearings in 2014, one of which lasted five days, at which what the Tribunal itself had described as "*the clarifying and collaborative value of adversarial oral* argument" was on public display. Sustained pressure from NGOs, concerned individuals and their advocates has led both to significant disclosures from security and intelligence agencies and to the uncovering of unlawfulness. In particular, and in recent weeks:

(a) The IPT ruled for the first time against the security and intelligence agencies on 6 February 2015, stating that prior to disclosures made during 2014, the regime governing the treatment in the UK of data obtained by the US pursuant to the Prism programme was not in accordance with the law, as required by Articles 8 and 10 of the ECHR.[122]

(b) A Code of Practice governing CNE was released on the same day, against the background of the *Privacy International* challenge to the use of CNE.

(c) The agencies conceded on 18 February that their policies and procedures relating to legal professional privilege had not accorded with human rights standards.

6.110. The IPT so confirmed in its *Belhadj* judgment of 29 April 2015, in the first judgment to find in favour of an individual against the security and intelligence agencies.

6.111. The IPT's procedure is different from an ordinary court procedure in a number of ways:

(a) Proceedings may on occasion be held in closed session without reporters and without the person who is raising the complaint attending the hearing. Alternatively, part of the hearing may be held in open and other parts in closed.[123]

(b) The IPT's decisions are normally only that it has made a determination in favour of, or against, the person complaining. The reasons for or explanation of the decision are not normally given.[124]

(c) There is no right of appeal against the IPT's decisions.[125]

(d) The IPT is not a "*senior court*" that has the power to declare an Act of Parliament incompatible with the ECHR, pursuant to HRA 1998 s4.

---

121 IPT/01/77, 9 December 2004.

122 [2015] UKIPTrib 13 77-H.

123 In practice, many complaints to the IPT do not result in a hearing but are disposed of on the papers.

124 The Tribunal has expressed doubts as to its capacity to grant relief (in the absence of undertakings) where there has been no determination in favour of a Claimant: Belhadj IPT Case, judgment of 29 April 2015, para 24(viii).

125 RIPA ss65-68.

(e) The IPT has the power to appoint a counsel to the Tribunal, who may hear the closed evidence and argue the case on behalf of the 'privacy' interests in issue. That stands in contrast to the special advocate regime in place for the Special Immigration Appeals Court.[126]

The Intelligence and Security Committee

6.112. The ISC is, as the name suggests, the parliamentary body tasked with providing oversight of the use of investigatory powers by the security and intelligence agencies (though not by other public authorities). It is a cross-party Committee, and its members are drawn from both the House of Commons and the House of Lords.[127]

6.113. It was recently reformed by the Justice and Security Act 2013 **[JSA 2013]**.[128] This made the ISC a full committee of Parliament for the first time, granted the ISC the freedom to choose its own chair, gave it greater powers and increased its remit. It now oversees the operational activity and wider intelligence and security activities of the Government. However, it is not responsible for reviewing ongoing and current operations being conducted by the agencies. The ISC's reports are submitted in the first place to the Prime Minister, who may redact any matters he considers should not be published.

126 On the role of the counsel to the tribunal, see the Liberty IPT Case, judgment of 5 December 2014, paras 8-10.

127 JSA 2013 s1(2).

128 Sections 1-4 and Schedule 1.

7. PRACTICE

Sources and scope

7.1. This Chapter describes how the powers outlined in Chapter 6 are used.

7.2. In relation to interception, it is based on written evidence provided by service providers and from each of the nine public authorities that are empowered to intercept communications. It is also based on oral evidence I received in the course of visits to each of the security and intelligence agencies, the NCA, MPS and the PSNI. I have also seen the highly classified material made available to the ISC for its parallel enquiry into privacy and security,[1] the confidential reporting to the Prime Minister by the IOCC and the ISCommr and closed material given by the Government to the IPT in the Liberty IPT Case.[2]

7.3. As to communications data, this Chapter is based in addition on written evidence from the police lead on communications data in England and Wales, Police Scotland, the Department of Work and Pensions **[DWP]**, the Local Government Association **[LGA]** and a number of other bodies that are empowered to obtain communications data. I received evidence from Royal Mail, whose powers to obtain such data has now been removed and from the Magistrates' Association. The Communications Data Strategy Group, a joint group of law enforcement and UK CSPs, held a special extended meeting for me at which I heard the views of CSPs and law enforcement representatives. I also visited NAFN in Tameside, and spoke to Gloucestershire and Nottinghamshire Police.

7.4. The evidence I received from the public authorities that use interception and communications data is mostly classified, since it sets out their operational needs and methods, and cannot be published. But I have seen and been able to discuss with security and intelligence agencies and other bodies some of their most sensitive capabilities and believe that I have a fair understanding of how they use the powers available to them.

7.5. Other types of investigatory powers (e.g. directed and covert surveillance and use of CHIS) fall outside the scope of this Review. But they are not so easy to separate out in practice: as demonstrated by a recent GCHQ publication,[3] information from a variety of sources must often be pieced together to achieve a comprehensive picture.

The Snowden Documents

7.6. Leaks of the Snowden Documents began to emerge in 2013 and continue to this day. Many of the published documents and slides refer specifically to GCHQ. The

---

1 The results of which are set out in the ISC Privacy and Security Report.

2 Though for the past two years, there have been no confidential parts to the reports by the IOCC.

3 "How does an analyst catch a terrorist?", an admirable (though inevitably limited) example of Agency transparency, which can be found on the GCHQ website: http://www.gchq.gov.uk/what_we_do/how_does_an_analyst_catch_a_terrorist/Pages/index.aspx.

Government has stated that at least 58,000 "*highly classified UK intelligence documents*" were among the documents stolen.[4]

7.7. The principal allegations broadly concern:

(a) Bulk collection of internet and international communications data;

(b) Analytic tools enabling advanced searching of intercepted data;

(c) Cooperative relationships between governments and service providers;

(d) Methods for CNE; and

(e) Intelligence sharing.

Some of these allegations are briefly summarised in Annex 7 to this Report.

7.8. It is important to note that:

(a) The British government has adopted an NCND approach to the allegations contained in the Snowden Documents (other than the PRISM programme, the existence of which has been acknowledged by the US government).[5]

(b) Only a tiny (and not necessarily representative) proportion of the Snowden Documents has been placed in the public domain.

The completeness and veracity of what has been revealed is therefore uncertain.

7.9. Nothing in this Report should be taken as confirmation by me that the Snowden Documents (or any of them) give a fair or representative view of the activities of GCHQ. Nor should I be taken to condone the activities of Edward Snowden.

7.10. But I have considered it important to refer to the allegations, because:

(a) it would be entirely artificial, and corrode public confidence in this Review, to proceed as if the disclosures had never been made or could be politely ignored; and because

(b) whether or not a true and fair picture is given by the limited selection of published documents and slides, it is clearly prudent to construct a regulatory system on the basis that programmes of the type described in these documents either exist or might in the future do so.

---

4 Deputy National Security Adviser Oliver Robbins, cited in "David Miranda row: Seized files endanger 'agents'", BBC website, 30 August 2013.

5 As can be seen from the Charles Farr Statement, para 41.

Interception

The uses of interception

7.11. Interception powers are summarised at 6.3-6.5, 6.10-6.15 and 6.34-6.59 above. Information on the use of interception powers is published each year in reports by the IOCC. In the Charles Farr Statement, the Director-General of OSCT set out the Government's view of the importance of intelligence obtained through interception:

> "Intelligence [from interception] has led directly to the prevention of terrorist attacks and serious crime, the success of operations aimed at countering the proliferation of weapons of mass destruction and the saving of lives. Overall, RIPA interception is a critical tool in investigations into the full range of threats to national security."

7.12. Many of the organisations empowered to use interception stressed to me its importance to the success of their work. For example:

(a) MI5 said that interception was "*a critical part of [their] toolkit*" used in a "*sizeable proportion*" of its recent investigations. "*In the majority of the operations in which it is used, interception of electronic communications provides unique intelligence which would be extremely hard, if not impossible to replicate through use of other sources*".[6] In 2013 this was estimated to be 15-20% of the total intelligence picture in counter-terrorism investigations.[7]

(b) The NCA told me that intercepted material "*is a key tool in the disruption of the most significant High Priority and Priority serious and organised criminals and their groups in the UK*. ... *For some areas of NCA activity ... there are no practical alternatives to using ... interception*".[8] In 2013-14, interception played a critical role in investigations that resulted in:

- Over 2,200 arrests;
- Over 750kg of heroin and 2,000kg of cocaine seized;
- Over 140 firearms seized; and
- Over £20,000,000 seized.[9]

(c) Police impressed upon me that intercepted material may be useful in other types of cases, ranging from corruption investigations to domestic murder.

6 Evidence to the Review dated 1 October 2014.
7 Home Office evidence to the Review October 2014.
8 Evidence to the Review dated 2 October 2014.
9 NCA performance data 2013-14 repeated in Home Office evidence to the Review October 2014.

This is notwithstanding the fact that in the UK, intercepted material (controversially, in the eyes of some) is not admissible as evidence in criminal proceedings.[10]

7.13. None of this is surprising: but it should not be assumed that interception is of universal utility. The chief terrorism investigator in the French judicial system said, of the Kouachi brothers who perpetrated the 2015 Charlie Hebdo shootings: "*The phone tapping yielded nothing. ... No one talks on the phone anymore.*"[11] Senior officers at Scotland Yard and the PSNI confirmed to me that there are hardened terrorists and organised criminals so security-aware that listening to their communications brings little reward.

Interception of known individuals

7.14. The vast majority of RIPA warrants issued (2,795 in 2014)[12] are made under RIPA s8(1). These are sometimes wrongly thought to deal only with internal communications i.e. those whose sender and recipient are in the "*British Islands*". In fact a s8(1) warrant may apply to all the communications of those named in the warrant. The use in principle of this form of interception, when targeted at individuals about whom there are grounds sufficient to make out a case for a personalised warrant, did not attract significant criticism from civil society groups or others who spoke to me.[13]

7.15. The question of "*thematic warrants"*, avowed by the ISC in February 2015 in the ISC Privacy and Security Report, was not addressed by those submissions, although I am aware that some may have concerns about such an interpretation of RIPA.

7.16. There were 1,585 s8(1) warrants in place at the end of 2014, of which "*the very significant majority*" related to a specific individual.[14] However:

(a) Where there is recognisable group of persons whose communications are to be targeted, it is permitted to include them all in one warrant even if not every member of the group can be identified in advance. These "*thematic warrants"* were viewed warily by the ISC, which wished them to be used sparingly and to be issued for a shorter duration than other warrants.[15]

(b) It is also possible that a single target might be subject to more than one interception warrant.

Accordingly, the number of warrants in place does not correspond to the number of individuals or investigations concerned.

---

10 *Intercept as Evidence*, (Cm 8989), (December 2014). A report by a Committee of Privy Counsellors led by Sir John Chilcott is the latest to recommend that arguments for change are not yet compelling. That report lists a further seven since 1993 which have reached the same conclusion. See also 9.16-9.18.

11 Marc Trévidic, quoted in "Gaps in France's surveillance are clear; solutions aren't", New York Times website, 17 February 2015.

12 Statistics on interception warrants are taken from *IOCC Report*, (March 2015).

13 There was however criticism of the fact that warrants are issued by the Secretary of State rather than an independent figure, and of the potentially wide definition of "*national security*".

14 ISC Privacy and Security Report, para 42.

15 ISC Privacy and Security Report, Conclusion D. Cf. *IOCC Report*, (March 2015), 6.71-74.

7.17. Of the warrants issued in 2014:

(a) 68% were issued on serious crime grounds,

(b) 31% were issued on national security grounds (which many of which would include terrorist investigations), and

(c) 1% were issued on a combination of grounds.

7.18. Some recent examples of the use of interception in the criminal sphere were published in December 2014, as part of the review of intercepted material as evidence.[16] They relate to the importation of Class A drugs, the supply and distribution of firearms, conflict between organised crime groups, money-laundering and fraud. They are reproduced at Annex 8 to this Report.

7.19. The Secretary of State for Defence gives the authority for interception by MoD under s8(1) warrants. This is a limited activity. The MoD conducts interception in the UK, targeted at its own communication, to enable equipment development and training for use in military operations. Material intercepted as part of a training activity is treated in accordance with RIPA s15 and deleted when it is no longer necessary or proportionate to retain it. Interception in the UK authorised by the Secretary of State for Defence may very rarely be needed to meet current military intelligence requirements.

Bulk interception

7.20. Bulk interception by GCHQ is used to support Government activities in the fields of foreign affairs, defence, including cyber defence, serious crime and counter-terrorism. It contributes to about 55% of the intelligence reports GCHQ produces.[17] The legal framework in which GCHQ operates and the applicable safeguards are summarised in Chapter 6: for a fuller treatment, the reader is referred to the very recent reports of the ISC[18] and IOCCO.[19]

7.21. A bulk warrant under RIPA s8(4) is targeted at a telecommunications system and therefore, in effect, targets communications bearers rather than specific, individual communications. There were 20 s8(4) warrants in place at the end of 2014. Interception under the WTA 2006 targets standalone communication systems such as those that may support military systems and private radio communications.

16 *Intercept as Evidence*.
17 Evidence from GCHQ, April 2015.
18 ISC Privacy and Security Report, chapters 4 and 5.
19 *IOCC Report* (March 2015), chapter 6. There is also fuller detail in the *IOCC Report*, (April 2014), sections 3 and 6.

The uses of bulk collection

7.22. The major use of communications collected in bulk is to detect or improve knowledge of threats to national security, which can then be subject to targeted examination. As the ISC put it:

> "GCHQ's bulk interception capability is used primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security. The people involved in those communications are sometimes already known, in which case valuable extra intelligence may be obtained (e.g. a new person in a terrorist network, a new location to be monitored, or a new selector to be targeted). In other cases, it exposes previously unknown individuals or plots that threaten our security which would not otherwise be detected."[20]

The importance of the "*target discovery*" described in the last sentence was particularly stressed to me by GCHQ.

7.23. This does not mean that suspicion plays no part in the selection of communication channels for interception, or in the design of the searches that are conducted on the collected material. Indeed the contrary is true:

(a) For reasons of resource constraint as well as proportionality, GCHQ considers carefully what communications channels it seeks to intercept and makes the case to the Foreign Secretary as part of the preparation for a bulk warrant issued under RIPA s8(4).

(b) The selection of targets whose communications are examined by agency analysts is controlled through an internal process which creates a permanent auditable record.

(c) The analyst must show the target to be relevant to the requirements set out in the certificate[21] which accompanies a s8(4) warrant, in effect one or more of the Government's PIC, and to meet a statutory intelligence gathering purpose, e.g. the interests of national security.

(d) The analyst must also demonstrate proportionality, typically by assessing the relevance of the communications to the intelligence requirement identified. Possible collateral intrusion is considered, for example the likelihood that a domestic fixed telephone line will have more users than the immediate target's email account.

---

20 ISC Privacy and Security Report, para 90. See, further, 14.43 below.

21 The ISC has recommended that the certificate be published, ISC Privacy and Security Report, Conclusion N. See 14.75 and Recommendation 43(b) below.

7.24. The ISC noted in March 2015:

> "We were surprised to discover that the primary value to GCHQ of bulk interception was not in the actual content of communications, but in the information associated with those communications."[22]

By "*the information associated with those communications*", the ISC was referring to both "*related communications data*" as defined in RIPA, and also to other content-derived information, relating for example to the characteristics of a communication, which is treated as content for the purposes of the law. This might for example be another email address used by a subject of interest.

7.25. GCHQ explained that its bulk access capabilities are the critical enabler for the cyber defence of the UK, providing the vast majority of all reporting on cyber threats and the basis for counter-activity. In a recent two week period bulk access provided visibility to GCHQ of 96 distinct cyber-attack campaigns. Bulk access is also the only means by which GCHQ can obtain the information it needs to develop effective responses to these attacks.[23]

7.26. GCHQ provided case studies to the ISC in order to demonstrate the effectiveness of its bulk interception capabilities. I have been provided with the same case studies and with other detailed examples, on which I have had the opportunity to interrogate GCHQ analysts at length and by reference to detailed intelligence reports based on the analysis of bulk data. They leave me in not the slightest doubt that bulk interception, as it is currently practised, has a valuable role to play in protecting national security. It does not of course follow that it is necessarily proportionate, which is for the courts to decide. I return to this topic at 14.39-14.55 below.

7.27. There are limits to what the public will (or should) take on trust. It is unfortunate, therefore, that the examples which the ISC gave to demonstrate the effectiveness of GCHQ's bulk interception capabilities had to be redacted from the open version of its report.[24] The six outline examples at Annex 9 to this Report go a little way towards remedying that defect. They illustrate the utility of bulk data capabilities more generally, particularly to identify previously unknown perpetrators of suspicious activity.

Interception capability and capacity

7.28. The Government has established a "*national authority*" for interception: the National Technical Assistance Centre [**NTAC**], which since 2006 is part of GCHQ. This was set up in 1999 by the Home Office, in the first place to assist law enforcement in the face of rapid technological change. It now supports all of the intercepting agencies, other than the MoD. About half of its funding still comes from the Home Office, and its work includes developing interception capabilities and infrastructure which are

22 ISC Privacy and Security Report, para 80.
23 Evidence from GCHQ, April 2015.
24 *Ibid.*, paras 82-89.

made available to the intercepting agencies. It interfaces directly with service providers.

7.29. GCHQ is responsible for developing NTAC's bulk interception and CNE capabilities.

7.30. Implementing a s8(1) warrant generally relies on the cooperation of service providers, acting typically in response to a direction from the Government under RIPA s12. A copy of the intercepted communication is passed by the companies to the intercepting agencies who examine it using their own staff and facilities. External communications may be obtained under a s8(4) warrant either directly by GCHQ, using its own capabilities, or through a service provider. Part of NTAC's role is to ensure that the needs of intercepting agencies can be addressed using the best available techniques, avoiding duplication of effort amongst the intercepting agencies whilst able to protect sensitive techniques that might be compromised by over-use.

7.31. In contrast to the position where communications data is concerned, there has been little discussion in recent years of the impact of technological developments on the feasibility of interception once it has been approved under warrant. Partly this reflects the sensitivity of the techniques used and the concern not to expose any weaknesses in them. Partly it reflects the continuing ability of the intercepting agencies, working with the service providers, to maintain access to communications channels. Nevertheless, the intercepting agencies acknowledge that the growth in the use of powerful encryption techniques, and their widespread availability from service providers or to individual users, undermines the historically high levels of probability that targets of interception identified in a warrant or Secretary of State's certificate will be able to be fully examined. A further powerful inhibitor on the ability to secure intercepted material is the increasing tendency to communicate using internet-based OTT applications, which are operated from overseas by companies which store data outside the UK. This is discussed at 6.95-6.99 above and 11.10-11.25 below.

Secretaries of State and WGDs

7.32. There are 18 Secretaries of State, all of whom may in theory issue warrants. In practice, other than in urgent cases when the usual Minister is unavailable, the Home Secretary deals with all warrants in Great Britain for MI5, the NCA, MPS and HMRC and any national security warrants from Police Scotland; the Secretary of State for Northern Ireland deals with applications in Northern Ireland and the Foreign Secretary deals with GCHQ and MI6 warrants. The Secretary of State for Defence deals with the small number of MoD warrants. These Secretaries of State also cover for each other's absence. The Cabinet Secretary for Justice in the Scottish Government deals with Police Scotland's applications to intercept in serious crime cases.

7.33. The Home Secretary has said that warrantry decisions occupy "*more of my time…than anything else*".[25] She dealt with the great majority of over 2,700 RIPA warrants that were handled by the Home Office in 2014, personally authorising 2,345 interception and property warrants and renewals during that year.

[25] Mansion House speech, 24 June 2014.

7.34. Before they consider a warrant, Secretaries of State receive advice from civil servants in the WGDs. The WGDs have what IOCCO has called a "*guardian and gatekeeper role*".[26] The majority of warrants are considered by the Home Office, in which the National Security Unit headed by a senior civil servant with 14 staff, provides round-the-clock support to the Home Secretary, and any other Secretary of State who is considering a warrant in her absence. The equivalent unit in the FCO the Intelligence Policy Department, is also headed by a senior civil servant and has two staff who support the warrant process and four more who may be involved from time to time. The Northern Ireland Office and Scottish Government have similar staff. Though subordinate to the approving Ministers, these are all independent of the warrant-seeking agency. They ensure that legal and policy advice on the warrant is taken where needed and that the warranty process is properly managed, including arranging, where justified, for the urgency procedures to be followed.

Handling of intercepted material

7.35. There are restrictions on the dissemination of intercepted material. These are set out in RIPA, ss15, 16 and 19, the Interception Code and in detailed arrangements drawn up for each intercepting agency and approved by the Secretary of State. Where possible only a summary and not the detail of intercepted communication should be disseminated. Intercepted material will often inform an intelligence report; but the raw material will be shared with as few people as possible.

7.36. Because intercepted material cannot be used in evidence, there is generally no need for it to be retained by the intercepting agency once its immediate use in providing intelligence is fulfilled. It is therefore destroyed at the end of the retention period, a process overseen by IOCCO.[27] There are number of grounds, largely concerned with oversight and audit, on which intercepted material can be retained for longer than the standard period.[28]

---

26 *IOCC Report*, (March 2015), para 6.48.

27 *IOCC Report*, (March 2015), paras 6.60-6.65.

28 These include:

- if the intercepted material continues to be, or is likely to become, necessary for any of the purposes set out in RIPA s5(3) – namely, in the interests of national security, for the purpose of preventing or detecting serious crime, for the purpose of safeguarding the economic wellbeing of the UK;
- if the intercepted material is necessary for facilitating the carrying out of the functions of the Secretary of State under RIPA Part I Chapter 1;
- if the intercepted material is necessary for facilitating the carrying out of any functions of the IOCC or the IPT;
- if the intercepted material is necessary to ensure that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution;
- if the intercepted material is necessary for the performance of any duty imposed by the Public Record Acts.

Communications data

7.37. The law relating to communications data is summarised at 6.6-6.8, 6.18-6.21 and 6.95-6.99 above. This section explains how in practice it is obtained, treated and used.

Retention and Acquisition of communications data

7.38. Communications data are produced and collected by service providers. Under data protection legislation, any personal data relating to their customers should be deleted as soon as it is no longer needed for their business purposes. However, DRIPA 2014 s1(1) grants the Secretary of State the power to issue a data retention notice to a service provider, requiring them to retain communications data, even if it is not (or was never) needed by the service provider. Before such a notice is given, the Secretary of State must take reasonable steps to consult with the service provider.[29]

7.39. When an investigating body wishes to secure access to those communications data, it will either authorise a person within the public authority to access the material or issue a notice to a service provider.[30] An authorisation provides for an individual within a public authority to obtain communications data. They are granted where a service provider is not capable of obtaining or disclosing communications data, where there is a pre-existing agreement in place with the service provider for disclosure or where it is not yet clear which service provider (if any) holds the data.[31] An authorisation is usually granted to a SPoC: they are most commonly used to access data via an automated system.[32]

7.40. A notice is served on a service provider asking it to disclose specified communications data.[33] Notices are typically served in cases where a service provider has not already been served with a data retention notice and there is no existing data acquisition framework. That is most likely to be the case with smaller service providers in the UK and with the overseas service providers. Overseas service providers often test whether they wish to comply with a notice by reference to their company practices and the laws of the jurisdiction in which the data is kept. I return to these issues at 14.58-14.59 and 14.78-14.86 below.

7.41. Authorisations and notices are valid for a month, but may be renewed.[34] They should be cancelled as soon as they are no longer needed.[35]

Authorising access to communications data

7.42. The mechanisms by which access to retained communications data may be authorised were set out at 6.64-6.70 above. For all but local authorities this is an

29 Retention Code, para 3.9.
30 Acquisition Code, para 3.2.
31 *Ibid.,* para 3.35.
32 *Ibid.*, para 3.35. These are known in the Code as "*Secure auditable communications data acquisition systems*".
33 *Ibid.*, para 3.43.
34 *Ibid.*, paras 3.51-57.
35 *Ibid.,* paras 3.58-64.

internal process with the input of a SPoC and final sign-off by a DP.[36] Following the *Digital Rights Ireland* judgment the requirement that the DP be independent of the investigation has been emphasised. It can be waived in cases, which must be explained to the IOCC, where the authority has only a small criminal investigation department or where there are ongoing operations or investigations immediately impacting on national security and an independent DP cannot be called upon.[37]

The use and impact of communications data

7.43. Communications data have become a basic tool in the investigator's armoury. There were 517,236 RIPA notices and authorisations, excluding urgent oral authorisations, in 2014, of which some 89% were issued by law enforcement and 10% by the Agencies.[38] But there are no statistics which set out the number of investigations in which it is used, or the number of people whose data were examined.[39]

Communications data and intelligence

7.44. MI5 explained to me that communications data allows it to be able to build a picture of a subject of interest's activities, and is extremely important in providing leads. It has had a significant role in every counter-terrorist operation MI5 has run in the past decade.[40] One of the advantages they identified was that analysis of communications data is a relatively speedy technique that allows targets to be identified for further work but may also help to determine that someone is of no further intelligence interest. For example, it may show that someone's contacts with a suspect are entirely innocent.

7.45. GCHQ makes extensive use of communications data to develop its intelligence picture, though much of its data is obtained as a by-product of its bulk interception of content: see 7.22 above.

7.46. The ISC summarised the manner in which the Agencies make use of communications data thus:

> "CD [communications data] is central to most Agency investigations. It is used to develop intelligence leads, to help focus on individuals who may pose a threat to the UK, to ensure that interception is properly targeted ... and to illuminate networks and associations relatively quickly. It can be particularly useful in the early stages, when the Agencies have to be able to determine whether those associating with the target are connected to the plot (and therefore require further investigation) or are innocent bystanders. GCHQ have established that they can analyse CD to find patterns in it that reflect particular online behaviours that are associated with activities such as attack planning, and to establish links."[41]

36 *Ibid.*, section 3.
37 *Ibid.,* para 3.13.
38 *IOCC Report*, March 2015, Annex B.
39 *Ibid.,* paras 7.29-31 set out the difficulties in establishing this information.
40 Evidence to the Review dated 1 October 2014.
41 ISC Privacy and Security Report, para 130.

Communications data and crime fighting

7.47. Communications data is used in the investigation of 90% of all serious crime, helping to establish who was (and was not) involved, with whom they acted and when and where they did so.[42] Some categories of crime, such as online crime, could not be investigated without it. In these cases they also provide an opportunity for law-enforcement to be proactive, looking for suspects, rather than waiting until a crime has been committed and a complaint made. That can contribute to the avoidance of harm rather than the crime solely being investigated afterwards. I am informed that communications data also play an increasing role across the range of criminal and missing persons investigations. A detailed picture of the utility of communications data in law enforcement is at 9.21-9.32 below.

7.48. One particularly controversial aspect of communications data use is the compulsory retention by service providers of data, now enshrined in DRIPA 2014. Retained data provides information about conduct in the past, often before a suspect is identified. It is frequently relied on to piece together conspiracies and associations between groups of criminals.

7.49. At Annex 10 to this Report are a number of examples of the use of retained communications data in the UK that were published by the European Commission.[43] The full document contains other examples of the use of retained communications data in other EU countries.

7.50. To understand and explain fully how communications data was used, the police carried out a detailed survey over two weeks in 2012 of the requests for communications data made by 62 law enforcement agencies nationally.[44] There is no reason think that this is an untypical period or that the results would today be significantly different. The major outcomes of that survey were:

(a) Communications data were requested for a very wide range of crimes. Almost a quarter of requests related to drug offences, but no other crime took up more than 11% of the total. A graphic representation of the crime types involved is at Annex 11 to this Report. 28% of data requests concerned people who were not suspects: 18% were victims.

(b) Almost a quarter of requests related to threat to life, an immediate risk or urgent operational necessity in relation to serious crime or national security: Annex 12 to this Report.

(c) 28% of all requests were for data over three months old. Older data was relied on particularly frequently in serious cases. 37% of data requests relating to sexual offences, 27% relating to terrorism, 11% relating to drugs, 5% relating

42 Evidence of the NCA to the Review. See also the range of uses of communications data highlighted in *IOCC Report*, March 2015, at 7.65 and 7.67.

43 DG Home European Commission, *Evidence for necessity of data retention in the EU* (March 2013), found at: http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf.

44 Evidence to the Review from the National Policing Lead for Communications Data, September 2014.

to homicide/attempted murder and 9% relating to firearms and explosives were older than six months.

7.51. Operation Notarise, a high-profile operation coordinated by the NCA offers a good example of the uses to which retained data can be put. It resulted in the arrest of over 600 suspected paedophiles who had been viewing indecent images of children. 3,982 requests for communications data were made as part of this operation, of which 3,646 (92%) were able to be resolved to identify a suspect. 336 of those requests were for data more than 12 months old which had not been retained.

Difficulties in obtaining data

7.52. Historically there has been a high availability of the communications data that investigators required. Typically the subscriber to a telephone number and the call log that went with it were the information needed; these were also the basis for the service provider to charge their customer.

7.53. The growth of internet-based services over the past twenty years has transformed that situation. Proliferating methods of communication, the fragmentation of providers, difficulties in attributing communications, changing business models and increasing use of overseas service providers have all tended to make data more difficult to access.[45]

7.54. The consequence is that to obtain the communications data needed for an investigation, even of one individual, a public authority may need to approach several service providers. The expertise of the SPoC in the investigating body is therefore of great significance in making an effective approach to a service provider. SPoCs know the right mix of service providers to approach and whether they are likely to have collected the data necessary to progress the investigation.

7.55. But however skilful their SPoCs, law enforcement bodies frequently complain of reduced access to communications data. This has led to pressure from law enforcement for legislation requiring service providers to retain more data (as in the draft Communications Data Bill of 2012), and also for action to facilitate the recovery of data from overseas providers (as in DRIPA 2014 s4, and pursuant to the initiatives that Sir Nigel Sheinwald was appointed to explore). I return to this subject at 14.23-14.28 and 14.58-14.59 below.

Use of communications data by local authorities

7.56. As set out at 6.67 above, local authorities are in a unique position when it comes to obtaining access to communications data. The term "*local authority*" does not distinguish between the different types of local authority (County, District, Unitary), which have very different enforcement functions. By way of illustration:

(a) Trading standards functions rest with a local weights and measures authority, which will generally be the local County Council or unitary authority.

[45] See 4.5-4.16 above.

(b) Environmental health functions (e.g. food hygiene, retail health and safety, noise nuisance, fly-tipping) rest with District Council.

Communications data is more likely to be useful in the enforcement of trading standards than it is in the context of environmental health.

7.57. A further complicating factor is the tendency since 2010 to centralise enforcement functions amongst authorities. In some cases, national specialist teams have been set up in local authorities: for example the National e-crime Team (based in North Yorkshire County Council trading standards department) and the National Illegal Money Lending Team for England (based within Birmingham City Council). There are also regional Scambusters teams to deal with enforcement in relation to such matters as doorstep crime and fraud.

7.58. As a result, it is necessary to approach any apparent trends in local government activity with caution.

7.59. Local authorities are only permitted to receive subscriber and service use data, whose principal use is in identifying a suspect from their telephone calls. Some examples of the use of communications data by local authorities are at Annex 13 to this Report.

7.60. NAFN is used by local authorities to provide a shared SPoC service from two centres in Tameside and Brighton. It was funded from 1997 by the DWP to strengthen the fight against housing benefit fraud. It continues to provide data and intelligence sharing and an investigatory educational service, encouraging the appropriate use of communications data to support investigations. Since 2008 it has provided a SPoC service under RIPA. NAFN is now funded by its members, 90% of which are local authorities, but it is open to all organisations which manage public assets. It continues to act as the authorising officer for obtaining communications data under the Social Security Fraud Act 2001 and other social security powers. It has been compulsory since 1 December 2014 for local authorities to use NAFN to obtain communications data under RIPA.[46]

7.61. I discuss the present and future use of communications data by local authorities at 9.96-9.100 below.

Computer network exploitation

7.62. As set out at 6.24-6.31 above, CNE was first avowed in the UK by the publication in February 2015 of the Draft Equipment Interference Code.

7.63. While no specific use is avowed in the Draft Equipment Interference Code, it is applied (by its para 1.6) to the following activities, any of which could (without authorisation under the ISA 1994) infringe the Computer Misuse Act 1990:

(a) obtaining information from equipment in pursuit of intelligence requirements;

46 Acquisition Code, para 3.86.

(b) obtaining information concerning the ownership, nature and use of equipment in pursuit of intelligence requirements;

(c) locating and examining, removing, modifying or substituting equipment, hardware or software which is capable of yielding information of the type described in a) and b); and

(d) enabling and facilitating surveillance activity by means of the equipment.

7.64. Some insight into the use of CNE was given by the Government in February 2015, in its open response to a case lodged at the IPT by Privacy International:

> "CNE operations vary in complexity. At the lower end of the scale, an individual may use someone's login credentials to gain access to information. More complex operations may involve exploiting vulnerabilities in software in order to gain control of devices or networks to remotely extract information, monitor the user of the device or take control of the device or network. These types of operations can be carried out illegally by hackers or criminals. In limited and carefully controlled circumstances, and for legitimate purposes, these types of operations may also be carried out lawfully by certain public authorities."

7.65. Privacy International (no doubt inspired by allegations in the Snowden Documents: see further at Annex 7 to this Report) had alleged in the same case that:

> "GCHQ has developed technology to infect individual devices, and in conjunction with the [NSA], has the capability to deploy that technology to potentially millions of computers by using malicious software ("*malware*")",

and described the use of such techniques as "*potentially far more intrusive than any other current surveillance technique, including the interception of communications*".[47]

Intelligence sharing

7.66. The international nature of the threats facing the UK mean that sharing intelligence with allies – including but not limited to its Five Eyes partners – is a fundamental part of the security and intelligence agencies' work.[48] The obtaining and disclosure of information by the security and intelligence agencies is governed by:

(a) SSA 1989 and ISA 1994,[49] which require the agencies to ensure that information is obtained and shared only in pursuit of their functions; and

(b) HRA 1998, which requires them to operate in conformity with ECHR rights including in particular Article 8.

---

47 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ and others*, Case No. IPT/14/85/CH **[PI IPT Case]** Statement of Grounds, paras 3 and 4.

48 ISC Privacy and Security Report, para 242.

49 Each agency relies upon a different statutory basis: SSA 1989 s2(2)(a) (for MI5), ISA 1994 s2(2)(a) (MI6), and ISA 1994 s4(2)(a) (GCHQ).

There is however no statute or Code of Practice governing how exchanges should be authorised or take place. The Government's position is that the routine sharing of intelligence reports and the more occasional sharing of raw, unanalysed intercepted material are governed, instead, by "*detailed internal guidance ... and by a culture of compliance*".[50]

7.67. The applicable arrangements were described in outline by the ISC in its recent report.[51] To summarise:

(a) No warrant is required to seek intelligence reports from overseas partners, though there are internal processes for verifying that the intelligence has been obtained in a manner compatible with the security and intelligence agencies' obligations under UK law.

(b) GCHQ has in practice always had an interception warrant in place for any raw intercepted material that it has sought from its overseas partners, and additionally (but voluntarily) applies the RIPA safeguards to all its data irrespective of how and under what authorisation regime it has been acquired.[52]

7.68. The Government's rationale for intelligence sharing was set out in the Charles Farr statement to the IPT (see 10.30).[53]

Bulk Personal Datasets

7.69. The use by the security and intelligence agencies of bulk personal datasets was publicly avowed only on 12 March 2015 when the ISC published its report.[54] I had already been extensively briefed on their use at all three agencies, and was also aware that the ISCommr has, for several years, been reviewing the use of bulk personal datasets as part of his duties.

7.70. I do not repeat the information contained in those reports, which is in every respect consistent with the information and demonstrations I was given.

The Management of Relationships with CSPs

7.71. Much of the Government, intelligence and police relationship with CSPs providers is conducted by NTAC. The Home Office has the lead responsibility for investigatory powers, sponsors the relevant legislation and guidance and is responsible for the payments to companies. The overall framework of legislation for the companies is however the responsibility of the Department of Culture, Media and Sport. There is an Interception and Communications Data Board chaired by the Home Office that coordinates work within the Government and warrant-requesting agencies on technical and policy issues. CSPs are not represented.

50 Charles Farr Statement, para 51.
51 ISC Privacy and Security Report, paras 247-254.
52 GCHQ evidence to ISC, July 2014.
53 Charles Farr Statement, paras 15-30.
54 ISC Privacy and Security Report, paras 151-163.

7.72. A Technical Advisory Board, set up pursuant to RIPA s13, brings together industry experts in a personal capacity, Government and agency representatives to advise the Home Secretary on the reasonableness of requirements imposed on companies to provide an interception capability. The Board does not have any regular meetings.

7.73. A Communications Data Steering Group, jointly chaired by industry and police representatives, provides a forum for the discussion amongst CSP representatives and some of the users of communications data. The group's role is entirely advisory.

7.74. There has been no similar group that examines interception issues from a multilateral perspective, though a Lawful Interception Strategy Group is being established at which Government, Agency and industry representatives will meet from May onwards.

7.75. None of these bodies has any representative of civil society groups. Furthermore, most of the evidence I received from CSPs observed there was an insufficient habit of communication and consultation between the Government and the companies on the policy for and practical impact of interference with communications for intelligence and investigation.

The Costs of Interception and Communications Data Use

7.76. Under RIPA s14, the Government must make a fair contribution towards the costs incurred by a service provider in implementing an interception capability, whether this is a standing capability required under s12 or just to give effect to a warrant, under s11. In practice this has been up to 80% of the capital cost of new interception capabilities and 100% of the ongoing operational costs. Where a service provider expands its network, it is expected to meet itself any increased capital costs of interception that arise.

7.77. The companies' capital costs are paid by the Home Office, the operational costs are met by the intercepting agencies based on the projected costs for the year ahead and apportioned to each agency based on relative usage. I was shown the costs of interception and asked not to publish them, in line with the Government's usual practice so that inferences cannot be drawn about the nature of these capabilities.[55]

7.78. The same reticence does not apply to publishing the costs of communications data used by public authorities. Grant payments to service providers to retain data were £13.5 million in 2013-14. Following the enactment of DRIPA 2014, grant payments are now made under the Data Retention Regulations 2014/2042. Public authorities also pay a charge for accessing communications data; these totalled £12.3 million in 2013-14.

55 Evidence from the Home Office, April 2015.

8. COMPARISONS

8.1. This Chapter offers some wider points of reference, to assist in evaluating the acceptability of intrusions into privacy and the manner in which they are authorised and reviewed.

8.2. The three comparisons I have chosen are:

(a) the use by public authorities of ***other forms of surveillance***: in particular, intrusive and directed surveillance and the use of CHIS;

(b) ***international comparisons*** for the regulation of investigatory powers; and

(c) the use of content and communications data by ***private companies***, in particular service providers.

8.3. None of these comparisons is exact, and there is insufficient space to develop any of them comprehensively here. But each of them provides a measure of perspective and can operate as a sense check when assessing the adequacy of the current law on investigatory powers, and when contemplating alternatives to it. This Chapter provides some basic information about each subject, and suggests some ways in which the comparisons may be instructive.

Other forms of surveillance

8.4. The main covert intrusive techniques used by the UK police and security and intelligence agencies, other than interception of communications and the examination of communications data, are directed and intrusive surveillance, property interference and use of CHIS.

8.5. Statistics on the use of the different intrusive techniques by law enforcement agencies are published by the OSC and are set out below.

8.6. The Intelligence Service Commissioner does not publish a breakdown for the use of such techniques by the Agencies and MoD. He gives the total of such warrants and authorisations – 1887 in 2013 – but said in his latest report that it was his view that disclosing details beyond this could be detrimental to national security.[1]

8.7. Opinions differ as to the relative intrusiveness of these powers: for example, we were told by the LGA that the OSC and IOCCO take different views concerning which powers should be used only as a last resort.

Directed Surveillance

8.8. Directed surveillance is observing someone covertly in a public place to gain private information about them in order to support an investigation. It is a power widely available to public authorities (comparable to those with access to communications data), is governed by RIPA Part II and RIP(S)A and is authorised within the public

[1] Report of the ISCommr for 2013, p. 35.

authority.[2] It is available for a broad range of purposes, reflecting the range of public authorities that are able to use the technique.

8.9. Directed surveillance, though covert like intrusive surveillance, differs from it in that it operates in a public place. It is also triggered by suspicion, and (as the name suggests) is practised in support of a specific investigation or operation.

8.10. In 2013-14, directed surveillance was authorised 14,076 times by law-enforcement bodies and other public authorities.[3] The Chief Surveillance Commissioner has noted a sharp decrease in the use of the technique by local authorities following the introduction of the requirement to obtain magistrates' approval. He did not necessarily attribute this to overuse in the past.[4]

Intrusive surveillance

8.11. Intrusive surveillance is covert surveillance carried out within a building or private vehicle. It is classically performed by attaching or embedding a device to record the activities of the individual or individuals under surveillance. It involves a high degree of interference with the right to respect for private life. Indeed, it might be characterised as more intrusive than interception of communications, on the basis that individuals have a greater expectation of privacy within their home than when using electronic communications such as mobile phones or email.[5]

8.12. Intrusive surveillance is available to similar bodies and for similar purposes to lawful interception. It is governed by RIPA Part II and RIP(S)A ss5-20. The Secretary of State has the power to authorise the intelligence services, an official of the MoD or a member of the armed forces to carry out intrusive surveillance.[6] The NCA, HMRC, police and Competition and Markets Authority **[CMA]** may be authorised to conduct intrusive surveillance by a Chief Constable or senior authorising officer.[7] A similar framework operates in Scotland, where police forces may be authorised to conduct intrusive surveillance by the Chief Constable of that force.[8] Except in urgent cases, a police, HRMC, NCA or CMA authorisation does not take effect until approved by a Surveillance Commissioner.[9] That Commissioner must have held judicial office.[10] The precedent of Commissioner authorisation for a highly intrusive power is one which I consider in the context of my recommendations in Chapter 15, below.

8.13. The police and other criminal investigatory bodies were authorised to carry out intrusive surveillance on 392 occasions in 2013-14.[11]

---

2 See RIPA ss28 and 30; RIP(S)A ss6 and 8.
3 OSC *Annual report of the Chief Surveillance Commissioner to the Prime Minister and the Scottish Ministers 2013-14*, paras 4.8-4.9.
4 *Ibid*, para 5.18.
5 Charles Farr Statement, para 29.
6 RIPA s41.
7 RIPA s32(6). A designated deputy may also grant an authorisation, s34(6).
8 RIP(S)A s10.
9 RIPA ss35(1) and 36(1); RIPA(S)A s3. An exception is made for cases that are urgent.
10 RIPA s63(2).
11 OSC, *Annual report of the Chief Surveillance Commissioner to the Prime Minister and the Scottish Ministers 2013-14*, para 4.6.

Property Interference

8.14. Intrusive surveillance will often depend on an entry being made into private property to place the device. As a result, the intelligence services or police may also require a property interference warrant, if they want to hack into a computer by physically modifying it.[12]

8.15. The security and intelligence agencies may be authorised to carry out property interference by a warrant issued by the Secretary of State under ISA 1994. As with intrusive surveillance, an authorising officer within the police may grant an authorisation to carry out property interference.[13] All such authorisations must be notified to a Surveillance Commissioner who subjects them to scrutiny.[14] Certain authorisations must be approved, rather than merely scrutinised after the event by the Commissioner: any authorisation to interfere with a dwelling house or office or that might provide access to confidential material.[15] This offers another example of Commissioner authorisation for a highly intrusive power, to which I return at 14.52 below.

8.16. Like intrusive surveillance, directed surveillance and CHIS, property interference is a covert technique that carries the risk of collateral intrusion. That collateral intrusion must be considered in advance before determining whether the interference with the right to respect for private life is necessary and proportionate. 2,689 authorisations to interfere with property were granted under the Police Act 1997 in 2013-14.[16] Some operations require property interference warrants in conjunction with other types of warrant, e.g. for intrusive surveillance or interception.

Covert Human Intelligence Sources (CHIS)

8.17. CHIS involves the use of agents, undercover officers or informants. A long list of public authorities are authorised to make use of CHIS, as set out in RIPA Schedule 2. A statutory instrument sets out which individuals within those bodies may authorise CHIS.[17] Within an ordinary police force, any superintendent may authorise CHIS. Local authorities may only obtain authorisations to carry out CHIS from a magistrate, following changes introduced by PFA 2012.[18]

8.18. Some argue that the infiltration of social networks by agents and informants is at least as intrusive as the interception of communications: yet whereas the latter requires the personal authority of the Secretary of State, the former (incongruously, it was said)

---

12 See 7.62-7.65 above.
13 Police Act 1997 s93.
14 *Ibid*., s96.
15 *Ibid*., s97. As with intrusive surveillance, there is an exception for urgent cases.
16 OSC *Annual report of the Chief Surveillance Commissioner to the Prime Minister and the Scottish Ministers 2013-14,* Appendix A.
17 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010SI 2010/521, as amended by the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013.
18 PFA 2012 s38.

used to require authorisation only by a superintendent and even now may be internally authorised by the police force concerned.[19]

8.19. Following public concerns about the long-term infiltration of an environmental protest group by officers, one of whom engaged in an intimate sexual relationship with an activist, a distinction has now been drawn between using undercover officers as sources and other forms of CHIS. Additional restrictions apply to the use of undercover officers. Thus:

(a) The use of undercover officers authorised by RIPA is now restricted to the police, NCA, Home Office and HMRC, and limited to match the responsibilities of those bodies.

(b) The use of undercover officers must be approved by an Assistant Chief Constable, even if (as is sometimes the case) the undercover deployment is intended to last only for a matter of hours).

(c) Long-term undercover operations (over a year) must be authorised by Chief Constable and then only with the approval of a Surveillance Commissioner.[20]

8.20. 4,430 CHIS were authorised in 2013-14 by law-enforcement bodies and other public authorities.[21]

8.21. The view was also expressed to me that there is no justification for the distinction that now exists between the authorisation of police and non-police informers, the intrusive effect of each operation being much the same. According to that view, the change to the rules for police informers in 2013 was a knee-jerk reaction which addressed the problem that had been in the headlines but did not look at the issues in a broader perspective.

Surveillance cameras

8.22. Surveillance cameras are widely used by public authorities for crime prevention and public safety. They include CCTV cameras in public places, automatic number plate recognition (ANPR) devices on roads and the body-worn video being introduced to police work. They are used more widely still by private individuals and businesses: the police estimated in 2011 that of the 1.85 million surveillance cameras in the UK, 1.7 million were privately owned.[22]

8.23. The use of surveillance cameras does not ordinarily require authorisation under RIPA: they are not used to carry out directed or intrusive surveillance because their use is overt, rather than covert.[23] Their use is regulated by DPA 1998 and PFA 2012. Two

---

19 Such arguments were emphasised in the submission of Birnberg Peirce & Partners on behalf of eight women who had been in intimate relationships with police officers.

20 The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013.

21 Report of the ISCommr for 2014, para 4.11.

22 JCDCDB Report, p. 7.

23 Covert Surveillance and Property Interference Code, para 2.27-2.28.

codes of practice have been issued in relation to CCTV.[24] PFA 2012 also established a Surveillance Camera Commissioner to oversee compliance with that Code and to review it from time to time. Where security companies operate cameras, whether on behalf of the public or private sector, the operators require a licence from the Security Industry Authority.[25]

8.24. Visitors from abroad are often struck by the quantity of CCTV cameras on British streets. Most of those whose activities are recorded are, of course, entirely innocent. Yet the cameras are not generally speaking a focus for resentment. CCTV evidence is routinely presented in certain types of criminal trial (e.g. for town centre assaults).[26]

8.25. Police forces also make increasing use of helicopters and drones that may carry cameras:

(a) RIPA and its codes of practice apply to any directed surveillance, whether it is carried out with the assistance of a surveillance device or other equipment, including aerial surveillance by helicopter or by use of remotely piloted aircraft systems (drones).

(b) Beyond directed surveillance, the use of airborne devices for surveillance is governed by regulations set by the Civil Aviation Authority, and is also subject to requirements on regulation of surveillance cameras under PFA 2012, along with DPA 1998 and the RIPA framework.

Use of bulk personal data

8.26. The ISC Privacy and Security Report revealed for the first time that the security and intelligence agencies make use of bulk personal data sets derived from information held by other public and private sector bodies.[27] The dealings of individuals with Government and non-governmental bodies are typically recorded in electronic databases. Those databases (which include passport application data) may be easily searched in order to obtain information about a particular individual or groups of individuals. Following this disclosure, the ISC recommended that the exercise of this power be formally overseen by the ISCommr and that recommendation was promptly accepted by the Prime Minister.[28]

8.27. There are a number of legal "*gateways*" under which data can be passed from the organisation which has collected it to another part of government.[29] This may be done

---

24 "In the Picture: A data protection code of practice for surveillance cameras and personal information" was issued by the Information Commissioner's Office **[ICO]** under DPA 1998. It sets out how individuals' privacy should be protected by the operators of surveillance cameras. The Surveillance Camera Code of Practice is issued under PFA 2012. It sets out Guiding Principles to govern the use of CCTV.

25 Private Security Industry Act 2001.

26 The presence of cameras is so commonplace that I have known a jury to ask, in such a case, why no CCTV material was put in evidence.

27 ISC Privacy and Security Report, Chapter 7.

28 Written ministerial statement by the Prime Minister, *Reports relating to the Security, Intelligence and Law Enforcement Agencies, and statutory direction to the Intelligence Services Commissioner*, (12 March 2015).

29 See, e.g., exemptions from the data protection principles set out in DPA 1998 Part IV, ISA 1994 s2 and SSA 1989 s2.

for example in the interests of national security or in certain cases for the prevention and detection of crime.

8.28. When material within those databases is aggregated, it becomes a powerful tool in the hands of security and intelligence agencies or investigators searching for suspect behaviour. One such system is HMRC's Connect database, described as a "*high-tech analysis system*" which allows, when combined with a "*wide range of data sources"*, the identification of "*evasion at the touch of a button"*.[30]

8.29. Big Data sets are also the basis for "*rules based targeting*". This technique involves the "*washing*" of relevant data against intelligence-led rules so as to identify passengers with a profile similar to those of known terrorists travelling on routes of concern. I have expressed the view elsewhere that this technique is an entirely useful and rational one for identifying travellers whom it may be appropriate to question, and if necessary to search, under the Terrorism Act 2000 Schedule 7.[31]

Enforced decryption

8.30. Where a device has been lawfully seized for examination and contains encrypted materials, the relevant authority can demand that the decryption key is handed over to enable all content to be examined.[32] This power, activated only in 2007, is highly intrusive but not covert. Any public authority that obtains unreadable material in the course of an investigation may seek the keys if it is necessary and proportionate to do so, but must first seek the concurrence of NTAC. Authority is given by a circuit judge for law enforcement agencies and by the Secretary of State for the agencies,[33] and the practice is overseen by the relevant Commissioners.[34]

8.31. Enforced decryption represents a possible way around the secure encryption of modern devices such as smart phones. However, as was pointed out to me, somebody whose device contains evidence which would be liable to convict him for serious criminality if it could be read might prefer to accept a relatively low prison sentence for refusal to hand over the encryption key. Enforced decryption was required 76 times in 2013-14, with two convictions in the same period for failure to comply.[35] I have previously drawn attention to the anomalous fact that the Code of Practice governing police port operations under the Terrorism Act Schedule 7 purports to permit them to demand the encryption key without reference to similar procedures or safeguards.[36]

30 https://www.gov.uk/government/policies/reducing-tax-evasion-and-avoidance/supporting-pages/preventing-tax-evasion.
31 D. Anderson, *The Terrorism Acts in 2013*, (July 2014), Annex 2, para 19.
32 RIPA s49.
33 See RIPA Schedule 2.
34 See RIPA s59(2), which grants the ISCommr the power to oversee the exercise by the intelligence services of all their powers in RIPA Part III, and RIPA s57(2)(c) which grants IOCC the power to oversee the exercise of RIPA Part II powers.
35 OSC Annual Report, September 2014, 4.13.
36 D. Anderson, *The Terrorism Acts in 2013*, July 2014, Annex 2 para 33.

Other intrusive powers

8.32. The JCDCDB in 2012 also drew attention, when considering other intrusive capabilities, to a number of mechanisms by which public authorities may obtain access to data on the basis of individual suspicion. Suspicious activity reports, arising out of financial and commercial transactions, are automatically reported to the NCA. The national fingerprints and DNA databases also contain many millions of entries.[37]

8.33. Securing access to this kind of data is relatively remote from the types of intrusion with which this Report is concerned. However, some parallels arise. For example, the *S and Marper* judgment of the ECtHR on DNA retention[38] has obvious implications for the retention of intercepted material and communications data.

8.34. Otherwise, as set out at 4.27-4.29, use may be made of OSINT, as to which there is some (although minimal) information in the public domain. Some techniques used by the private sector to gather information are set out in at 8.65-8.83 below.

Measuring Intrusion

8.35. Opinions differ as to the relative intrusiveness of these various techniques. Relevant factors include whether they operate in a public, private or electronic space (which may affect an individual's expectations of privacy), whether they involve deception (CHIS); and their capacity to operate in bulk (CCTV) or only on suspicion (intrusive and directed surveillance).

8.36. The levels of authority required before these powers may be exercised imply a broad parity between:

(a) interception of communications, intrusive surveillance and property interference; and

(b) requests for communications data, directed surveillance and CHIS.

Recent legal changes prompted by prominent news stories have reflected shifts in the public perception of how intrusive these powers are. Most notably, the level of authorisation required for police CHIS and for local authority requests for communications data have been increased.

8.37. A more formal structure (or "*ladder of escalation*") for evaluating the relative intrusiveness of surveillance methods has been proposed by Professor Ross Bellaby, acknowledging the influence of Sir Michael Quinlan, Sir David Omand and others.[39] Another "*matrix"* of surveillance technologies has been developed by SURVEILLE, a project funded by the European Commission.[40]

---

37 JCDCDB Report, p 7.

38 *S and Marper v UK* (Application nos. 30562/04 and 30566/04, judgment of 4 December 2008).

39 R. Bellaby, *The Ethics of Intelligence*, 2014.

40 SURVEILLE, *Paper Assessing Surveillance in the Context of Preventing a Terrorist Act,* (May 2015) **[SURVEILLE Report]**. See further 14.44(a) below.

International Comparisons

8.38. Comparing the UK's legal regime with those of other countries is fraught with danger, for a number of reasons:

(a) The UK is far from unique in the complex and fragmented nature of the law governing investigatory powers. I had the impression that in many countries, the number of people professing fully to understand the relevant law, even among academics and the legal profession, was remarkably small.

(b) By focussing only on what is written on the page, the observer risks failing to appreciate other aspects of how things operate in practice. Intelligence agencies everywhere in the world operate largely in secrecy, for obvious reasons. It cannot be excluded that practices take place which are completely unknown to commentators or which have no legal sanction whatsoever (as was the case with phone tapping in the UK prior to IOCA 1985).

8.39. But a comparative picture, however imperfect, is desirable. I have attempted to make some comparative observations in respect of lawful interception, access to communications data and communications data retention (amongst other topics). However, this Chapter does not offer anything comprehensive or authoritative. In the course of preparing it, I have drawn on published comparative surveys, on my own visits to the US, Canada and Germany and on assistance kindly given by national experts to address some issues of particular interest.[1]

Five Eyes partners

8.40. UK security and intelligence agencies, together with their counterparts in Australia, Canada, New Zealand and the USA, form part of the Five Eyes partnership – a grouping which had its origins in the 1946 UKUSA information-sharing agreement, declassified in 2010.[2]

8.41. Each of the Five Eyes is a common law jurisdiction that shares at least some elements of its legal heritage with the UK. As a result, the laws of the other Five Eyes members provide a particularly useful comparator. I have briefly summarised the law of interception and access to communications data in each of the Five Eyes states in Annex 15 to this Report.

Content and communications data

8.42. The precise boundaries between communications data and content are not defined in the same manner around the world. However, there appears to be a broad consensus that the content of a communication falls into a different category from data relating to communications. As set out in Annex 15 to this Report, a number of the other Five

1 In particular David Medine (PCLOB) and Alan Butler (EPIC) from the US, Prof. Craig Forcese from Canada and Prof. George Williams and Kieran Hardy from Australia.

2 See http://www.nationalarchives.gov.uk/ukusa/.

Eyes partners have recently moved to clarify their definition of communications or call associated data.[3]

Authorisation

8.43. Many states provide different authorisation pathways for law enforcement on the one hand and security and intelligence agencies on the other. In some, though not all, states those differing frameworks are set out in separate statutory regimes.

8.44. In contrast to the UK position, criminal law enforcement bodies in the United States, Canada, Australia and New Zealand must all obtain judicial authorisation before they carry out interception.[4]

8.45. The position in terms of police access to communications data/metadata is more complex. In Canada and Australia, some form of judicial authorisation is required before the police may access metadata. In the United States, federal law enforcement agencies such as the FBI may access metadata without judicial authorisation, but State police forces ordinarily require a subpoena or a court order in order to do so.[5]

8.46. As to the security and intelligence agencies of the Five Eyes partners, the US intelligence agencies may apply to a specialised federal court, the Foreign Intelligence Surveillance Court **[FISC],** in order to receive authorisation to collect intelligence material. However, Executive Order 12333 **[EO 12333]** also provides the power to intercept communications without judicial oversight.[6] The Canadian Security and Intelligence Service **[CSIS]** require both Ministerial and judicial authorisation (from a special bank of Federal Court Judges) before they may carry out interception. However, the Communications Security Establishment **[CSE]**, which obtains foreign intelligence outside Canada, may carry out overseas interception without prior judicial approval.[7] The structure in New Zealand is very similar to that in Canada. The New Zealand Security and Intelligence Service **[NZSIS]** must obtain the approval of a minister and a retired High Court judge, if it wishes to carry out interception inside New Zealand. Foreign intelligence warrants may be authorised by the minister alone.[8] The Australian Security Intelligence Organisation **[ASIO]** may be authorised to carry out interceptions by the Attorney General.[9]

---

3 New Zealand: Telecommunications (Interception Capability and Security) Act 2013 **[TICSA 2013]** established a new statutory definition of "*call associated data*". Australia: a new mandatory data retention regime specifies categories of information that must be kept by service providers for a period of two years. Canada: The Protecting Canadians from Online Crime Act 2014 **[PCFOC 2014]**, defined "*tracking data*" and "*transmission data"* (Canadian Criminal Code para 487.011). USA: "*Intercept"* has been defined since the 1968 under the Wiretap Act **[WA 1968]:** the "*aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device*".

4 See paragraphs 80-84, 34-38, 8-13 and 68-72 in Annex 15 to this Report.

5 See paragraphs 85-86, 38, 17-24 and 73-75 of Annex 15 to this Report.

6 See para 102 of Annex 15 to this Report.

7 See para 54 of Annex 15 to this Report.

8 A similar mechanism applies to the Government Communications Security Bureau **[GCSB]**. See paragraphs 64-67 of Annex 15 to this Report.

9 See paragraphs 3-7 of Annex 15 to this Report.

8.47. As is clear from the above, the UK is unique in the Five Eyes in making no use of judges for the prior authorisation of interception warrants. But there is no single standard applied by the other members.

8.48. In Europe, judicial authorisation is not universal:

(a) In Germany, the position of the security services remains essentially as it was described by the ECtHR in the case of *Klass v Germany.* After an initial control by "*an official qualified for judicial office*", interception warrants are approved by the G-10 Commission, a committee of present and former members of parliament which meets monthly. The ECtHR, whilst noting that "*it is in principle desirable to entrust supervisory control to a judge*", rejected the submission that this was an unacceptable "*form of political control*".[10] Law enforcement agencies require a court order before they are entitled to carry out interception.

(b) The situation in the Netherlands is in flux. As outlined at 5.50-5.74 above, the Dutch Data Retention Law was declared unlawful by the District Court of the Hague in March 2015. A previously-proposed draft bill, which would require police and public prosecutors to obtain judicial authorisation before securing access to communications data retained by CSPs, may be relied upon by the Dutch Government to remedy the position.[11] The Dutch Security Services currently have the power to intercept communications without judicial authorisation, on the authority of either the Minister of Interior or the Minister of Defence.[12]

(c) In France, a new Intelligence Bill, introduced in March 2015 will if passed put the powers of the security services to carry out interception and gain access to communications data on a statutory footing.[13] Currently the exercise of security service powers in that area is subject to review by a 3-person interception committee. The new Bill will allow for intelligence service warrants to be authorised by a Minister but scrutinised by an independent oversight committee of nine people including judges, MPs and IT specialists. That body would have the power to refer authorisations to the *Conseil d'État* if it considered they were irregular.[14]

8.49. A 2011 European Commission evaluation of the Data Retention Directive (Directive 2006/24/EC) set out the various routes by which access to communications data might be secured in different countries:[15]

(a) Purely judicial (magistrate or judge): Denmark, Greece, Spain, Netherlands;[16]

---

10 Paras 20 and 54-56.

11 See however the open advice of the Dutch Data Protection Authority, available online in Dutch https://cbpweb.nl/nl/publicaties/wetgevingsadviezen.

12 State Security Act (*Wet op de inlichtingen – en veiligheidsdiensten)* 2002, Article 25.

13 Draft Police and Security: Information Bill, published on 19 March 2015.

14 *Ibid.,* para 2.

15 Com(2011) 255 final, 18 April 2011, pp. 9-10.

16 The position in Finland is that no authorisation is required for subscriber information but judicial authorisation is required for traffic data.

(b) Judicial or prosecutor: Belgium, Cyprus, Netherlands;

(c) Public prosecutor alone: Italy, Hungary;

(d) Public prosecutor or police: Latvia, Slovakia;

(e) Police authorisation: Ireland; Poland;

(f) Senior official in Ministry of Interior: France.

Oversight

8.50. Various published documents purport to compare the oversight regimes of different states:

(a) A Report produced by the University of Durham and the Parliament of Norway in 2005, with summary table comparing the position in eight countries.[17]

(b) Annex B to the UK Parliament's Home Affairs Select Committee's *Counter-Terrorism* Report, which sets out the comparative oversight frameworks in the UK and the US.[18]

(c) A document from the New Zealand Parliament, comparing the oversight regimes in the UK, New Zealand, Australia and Norway.[19]

(d) Annex 1 to a 2013 report of the European Parliament on mass surveillance, comparing the legal position in the UK, France, Germany, Sweden and the Netherlands.[20]

8.51. A brief review of the Five Eyes partners demonstrates that they have all established at least some element of oversight by the legislature, as well as scrutiny by a Commissioner or Inspector-General.

8.52. Both the Australian and New Zealand Inspectors General have a broad mandate with a strong investigatory function.

8.53. The Canadian Security Intelligence Review Committee **[SIRC]** combines both parliamentary and external review within one entity. The members of the Committee are parliamentarians, but much of the practical day-to-day operational work is carried out by the employees of SIRC. The appointed members only meet on a small number of days per year. CSE is overseen by a special Commissioner, a retired judge, who reports on the interceptions granted by the Minister on an annual basis.

8.54. As well as a permanent select committee on intelligence in both Houses of Congress, the United States has a variety of oversight mechanisms. The Privacy and Civil

17 H. Born and I. Leigh, *Making Intelligence Accountable,* (2005) accessible at: http://www.dcaf.ch/Publications/Making-Intelligence-Accountable.

18 17th Report of Session 2013-14, HC231 (May 2014).

19 New Zealand Parliament, "External oversight of intelligence agencies", May 2013.

20 European Parliament Directorate-General for Internal Policies, "National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law", 2013.

Liberties Oversight Board provides advice and oversight to the US Government on questions of terror prevention. A separate President's Intelligence Oversight Board reports directly to the President on potential violations of the law. Many of the Agencies themselves also contain an Office of Inspector General, with a remit to review compliance internally.[21]

Data Retention

8.55. The European picture concerning data retention is diverse and complex. Prior to the decision in *Digital Rights Ireland*, the EU Data Retention Directive required Member States to pass laws requiring the retention of certain metadata for between 6 and 24 months.

8.56. An opinion by the European Parliament's Legal Service concerning European data retention post-*Digital Rights Ireland* appeared in January 2015.[22] It listed the Member States whose courts had annulled data retention laws prior to the *Digital Rights Ireland* judgment (Bulgaria, Romania, Germany, Cyprus, Czech Republic), as well as the first three to have done so since (Austria, Slovenia, Romania), and concluded that Member States which wish to retain data retention laws must ensure that they comply with EU law.

8.57. A very full summary of EU data retention laws in the EU Member States was published by the Open Rights Group in April 2015.[23]

8.58. As to the Five Eyes partners, both Canada and Australia have recently passed legislation to require telecommunications providers to retain some data.[24] Telecommunications providers in New Zealand are already required to be capable of obtaining call associated data and to provide it to police and security services when served with a warrant.

8.59. An important distinction between US and UK law (as it currently stands) is that there is no requirement for CSPs in the United States to store data beyond their own business needs. On the other hand, US CSPs are not obliged, as are their European counterparts, to delete or anonymise data once it is no longer necessary for business purposes. I was informed during my trip to the US that it was highly unlikely that Congress would consider legislation requiring service providers to retain or create data that they did not themselves need for business purposes (such as billing). However, CSPs are required to retain data that they already produce and create such as name, address, telephone number of the caller, telephone number called, date, time and length of a call.[25]

---

21 17th Report of Session 2013-14, HC231 (May 2014), p. 92.

22 Legal Opinion to LIBE, which can be accessed at: https://s3.amazonaws.com/access.3cdn.net/27bd1765fade54d896_l2m6i61fe.pdf.

23 Open Rights Group, "Data Retention in the EU following the CJEU ruling", (April 2015).

24 Australia: Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015. Canada: PCFOC 2014.

25 Under 47 C.F.R. § 42.6.

Bulk Collection

8.60. A comparative picture of bulk data collection and data analysis is very difficult to provide. Many states do not officially avow their bulk data programmes (if they exist) and have continued this practice in the light of the disclosures in the Snowden Documents.[26]

8.61. Furthermore, legislation does not ordinarily describe bulk collection powers in terms. By way of example, RIPA s8(4) is not described as a mechanism for bulk collection, though in practice that is one of the uses to which it is put. Nonetheless, it is clear that an Australian foreign communications warrant, issued under the Telecommunications (Interception and Access) Act 1979 **[TIA 1979]** ss11A, 11B or 11C, will allow for bulk collection. Likewise the GCSB in New Zealand may obtain an access authorisation warrant that enables it to access specified information infrastructures (with no greater degree of specificity required).[27] It is also clear that the Canadian CSIS and CSE carry out large scale data analysis. For its part, the US Government has officially avowed its PRISM programme, which involved the collection of large volumes of data by the NSA.

8.62. As to the various European states, the new French Intelligence Bill would grant the Prime Minister the power to require CSPs to monitor communications data passing through their networks on a purely anonymous basis. If the data patterns are suspicious, the CSP may be required to "*de-anonymise*" that data.[28] It also provides for the bulk interception of communications "*sent or received abroad*."[29]

8.63. The Venice Commission Report of April 2015 explains that both Germany and Sweden make statutory provision for bulk interception.[30] The Snowden Documents suggested that the German external intelligence service (BND) passed very large volumes of metadata to the NSA.[31] The Dutch Government is currently debating a revision to its Intelligence and Security Act 2002. It is unclear whether the final form of that revision will allow for bulk interception of external communications and on what basis.

8.64. Bulk collection is, at least presently, a reality of the surveillance landscape, at least when carried out for the purposes of foreign intelligence, and conducted outside the state concerned.

---

26 See however I. Brown and others, "Towards multilateral standards for surveillance reform": https://cihr.eu/wp-content/uploads/2015/01/Brown_et_al_Towards_Multilateral_2015.pdf.

27 GCSB Act s15A (1).

28 Intelligence Bill 2015 L. 951-4.

29 *Ibid.,* L. 854-1.

30 Venice Commission Report, p. 27, fn 81.

31 *Der Spiegel,* 5 August 2013. A German Parliamentary Committee has been set up to investigate the matters arising from the Snowden Documents, though its focus is on questions concerned with spying carried out by other states in Germany. See "German BND spy agency helped Germany target France", BBC website 30 April 2015.

Private sector activity

How private companies operate

8.65. It is barely possible to engage in everyday social and economic activity without consenting to the handover of private information to private companies and at that point losing some control over how it is used.

8.66. Service providers, (particularly online social networks), retailers and others hold vast amounts of commercially valuable data about individuals, which can be monetised in a host of ways, such as credit reference checks and targeted advertising on the internet.[1]

8.67. Services which are free to customers on the internet are generally paid for by the ability of companies to exploit the data that the customer's interaction with them creates: everything from buying habits to location and movement and social preferences. For example:

(a) Google combines data from a range of sources to display advertising most likely to generate advertising revenue. Google's online terms of service state "*Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.*"[2] Sources can include a user's IP address, Google and Youtube profiles, Google search engine results, Google map requests and apps belonging to businesses which advertise with Google. Google offer their "*partners*"[3] a number of products to help manage their advertising and websites, including "*Adsense, Adwords, Google Analytics and a range of DoubleClick-branded services*".[4]

(b) According to Facebook's 2015 Data Policy it "*shares*" information about users "*within the family of companies that are part of Facebook"*.[5] This may be done to "*facilitate, support and integrate their activities.*"[6] There are currently ten companies listed in the family, including Whatsapp, Instagram and Atlas (an advertising platform, aimed at helping companies track the effectiveness of online ads). Facebook's Audience Network programme provides app developers with aggregated data to target their ads. "*Facebook Services*" are also covered by this Data Policy and include Services such as "*Audience Insights*". This service is designed to provide businesses with information about the "*geography, demographics and purchasing behaviour and more*"[7] of their target audiences. In March 2015, Facebook launched Topic Data in the UK

1 "How Wireless Carriers are Monetizing Your Movements", MIT Technology Review Website, 12 April 2013.
2 See http://www.google.com/intl/en/policies/terms/.
3 A list of partners is not provided, see http://www.google.com/policies/privacy/example/our-partners.html.
4 See https://www.google.com/intl/en/policies/technologies/ads/.
5 See https://www.facebook.com/about/privacy/update.
6 See https://www.facebook.com/help/111814505650678.
7 See https://www.facebook.com/business/news/audience-insights.

and US. This provides select access to advertisers about the topics being discussed by Facebook users.

Data brokers

8.68. Data brokers are companies which collect consumers' personal information and resell or share that information with others. They collect this information from commercial, government and publicly available sources, often analysing it to make certain inferences about customers before selling it to clients. Examples of data brokers include Datalogix and Acxiom.[8]

8.69. The lack of transparency relating to this type of company led to a study of nine data brokers by the Federal Trade Commission in the US in 2014. The study found:

> "Data brokers acquire a vast array of detailed and specific information about consumers, analyze it to make inferences about consumers, some of which may be considered sensitive; and share the information with clients in a range of industries. All of this activity takes place behind the scenes, without consumers' knowledge."[9]

8.70. Specific findings included that seven out of the nine data brokers shared data with other data brokers providing "*a detailed composite of the consumer's life.*"[10] The database of one of the data brokers investigated covered one trillion dollars in consumer transactions.

8.71. In April 2015, the ICO launched an investigation into UK firms sharing pension, medical and financial data.[11]

Data protection

8.72. The rules and guidance set out in DPA 1998 and consumer protection law are intended to protect individuals from unfair use of such data. However, the House of Commons Science and Technology Committee recently expressed doubt about the ability of current legislation to deal with data passing over digital platforms.[12] A draft EU Regulation and Directive, introduced in 2012 with the aim of providing rules "*to catch up with the digital age*", are still being negotiated by Member States.[13]

---

8 *Data Brokers: A Call for Transparency and Accountability* (May 2014).

9 *Ibid*., p. vii.

10 *Ibid.,* p.11.

11 See the announcement on the ICO website: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/04/ico-to-make-enquiries-about-sale-of-pension-data/.

12 *Responsible Use of Data*, HC 245 (November 2014), p. 3.

13 See the European Commission Factsheet, "Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market", 28 January 2015. The CMA is currently carrying out an inquiry into a number of issues relating to the commercial use of consumer data, including consumer understanding about the collection of data and how consumer data are aggregated, bought and sold.

The impact and extent of commercial use of consumer data

8.73. Commercial use of consumer data can have serious impacts on the personal lives of individuals:[14]

(a) A woman's sexuality was exposed to her colleagues, against her wishes, because of the advertisements that popped up on her screen.[15]

(b) A department store sent coupons for baby items to customers whose purchasing history gave them a high "*pregnancy prediction score*". The father of one teenage recipient made a complaint to the department store before discovering the accuracy of the prediction.[16]

(c) A credit card company lowered a customer's credit rating because he shopped at places where other customers had a poor repayment history.[17]

8.74. Moreover, such use of data is increasingly complex:

(a) A Canadian firm tracks up to 10 million mobile devices every day in Toronto and builds lifestyle categories based on people's movements.

(b) Shoppertrak uses in-store WiFi sensors to track customers' phones so it knows if they return to the store.

(c) At least 160 third party websites watch the users of OKCupid, a dating site, noting the websites they visit later.

(d) Various identification technologies are in development. As well as the familiar (and fast improving) facial recognition systems, these include voiceprint recognition systems, iris scanners that work at distance, gait recognition systems and systems for identifying people by typing style, writing style and even – apparently – body odour.[18]

8.75. The significance of such developments is expressed in the following prediction:

> "Store clerks will know your name, address, and income level as soon as you walk through the door. Billboards will know who you are, and record how you respond to them. Grocery store shelves will know what you usually buy, and exactly how to entice you to buy more of it. Your car will know who is in it, who is driving, and what traffic laws that driver is following or ignoring."[19]

---

14 The examples in this section are taken from M. Venkataramanan, *My Identity for Sale,* unless otherwise stated.

15 J. Angwin, *Dragnet Nation: A quest for privacy, security and freedom in a world of relentless surveillance*, 2014, p. 167.

16 "How Companies learn your secrets", The New York Times Magazine, 16 February 2012.

17 A. Croll,"Big Data is our Generation's civil rights issue, and we don't know it", Solve for Interesting website, 31 July 2012.

18 B. Schneier, *Data and Goliath*, 2015, chapter 2.

19 *Ibid*.

The author adds that while at present "*many of our surveillance systems are still visible to us*" more of those systems are likely to become hidden in the future.

8.76. Sensing the force of such points, modern dystopian literature (in contrast to *Nineteen Eighty-Four*) tends to focus at least as much on the evils of the (private sector) "*surveillance society*" as on those of the (more extensively regulated) "*surveillance state*".[20]

Tracking methods

8.77. As is clear from the above, a significant tool in a private company's armoury is the tracking of communications online. Digital advertising provides a significant method of tracking, as well as presenting a quantifiable return on investment. It takes place via an increasing number of methods.

Cookies

8.78. Cookies are small text files placed on a computer's hard drive when a browser visits a website. They work in conjunction with pixel tags to notify a website that a visit has previously taken place. They include:

(a) ***First party cookies***, sent by the website a browser is visiting.

(b) ***Third party cookies***, sent by a website other than the website the browser is visiting. For example, an advertisement appearing on the website can send a third party cookie, thus allowing the network managing the third party cookie to track information about a user's browsing habits and engage in targeted advertising.

(c) ***Zombie cookies*** or ***super cookies***, which reappear after they have been deleted by a user.

(d) ***Cookie-syncing***, which is the practice of third party websites linking IDs allocated to a user. This can improve tracking, particularly when used in conjunction with zombie cookies.[21]

8.79. The rapid growth in ownership of mobile devices has meant that companies have had to find alternative methods to carry out tracking: cookies are not shared between apps and so have limited value on mobile devices. A number of methods have been adopted to overcome this problem:

(a) ***Single Sign On*** permits a user to enter one name and password in order to gain access to multiple applications. For example, a Facebook ID can be used to log

[20] See e.g. Dave Eggers' 2014 novel *The Circle* and cf. James Graham's play *Privacy*, which sold out the Donmar Warehouse in London in 2014.

[21] G. Acar et al, "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild", (2014) Proceedings in the CCS, p. 681.

into third party websites, allowing Facebook to collect information about users' visits to these third sites.[22]

(b) ***Header enrichment*** refers to the process of injecting a number into a HTTP header each time a user visits a website.

(c) ***Fingerprinting*** techniques collect different pieces of information relating to a device or browser to enable identification.

Deep-linking

8.80. Approximately 90% of the time spent using mobile devices is spent in apps.[23] Apps do not follow the structure of the web and so the usual tracking methods are not available. Deep-linking allows app developers to link to pages in apps and so replicate the structure of the web and enable tracking.

Social plug-ins

8.81. Social plug-ins facilitate the sharing of third party content within online social networks. Examples include Facebook's "*like*" button, Google+'s "*+1*" and Twitter's "*tweet*" button. When a person visits a third party webpage in which a plug-in is embedded the domain of the plug-in provider may receive certain information automatically. This is examined in more detail at 8.100 below.

Adware

8.82. Adware is used to describe software which is embedded with advertisements. It is commonly used to allow users to have access to software without having to pay for it. However, adware software may also track web browsing habits in order to facilitate targeted advertising by third parties. This practice is a form of spyware.

Location Tracking

8.83. "*Passive location tracking*",[24] (when an application collects location data even when it is not in use), is increasingly common: the Angry Birds app provides it. A further trend is the growing use of location-tracking to enable targeted advertising. In 2014, Facebook launched Local Awareness ads. Advertisers can target their advertisements to users who are near their business.[25]

Protections

8.84. There have been three core strategies used to combat private companies' collection and use of data and to ensure privacy online: individual notice and consent, opting

22 See Facebook's Data Policy: https://www.facebook.com/about/privacy/your-info-on-other#instantpersonal.
23 "Getting to Know you", The Economist, 13 September 2014.
24 "Location-tracking: 6 Social App settings to check", Information Week, 26 August 2014.
25 See https://www.facebook.com/business/a/local-awareness.

out and anonymisation. However, these have arguably now lost much of their effectiveness.[26]

Consent

8.85. The significance of online consent can easily be over-stated. The issue in the context of social media platforms was examined by the House of Commons Science and Technology Committee. Witnesses observed that signing forms "*is often not an act of informed consent*",[27] that "*people need to know what they are signing up to*",[28] and that "*everyone clicks 'Yes'*".[29] Witnesses were particularly critical of the complexity of terms and conditions, describing them as "*more complex than Shakespeare*".[30] The Committee concluded that "As a *mechanism for showing users have provided informed consent, so that organisations can process incredibly personal data, terms and conditions contracts are not fit for purpose".*[31]

8.86. In 2014, the Article 29 Working Party suggested that Google amend its privacy policy so as to avoid "*indistinct language*" and obtain consent "*in a clear and distinct manner".*[32] A study of Facebook's 2015 Data Policy concluded that it was unclear "*to what extent user data is shared with other entities such as 'Facebook Companies', 'Third Party Partners' and 'Customers', nor what the exact identity is of these entities".*[33]

8.87. There have been some changes: following an ICO investigation and negotiation with Google, which concluded that Google's privacy policy did not give enough information to customers on how and why their data was collected, the ICO said:

> "This investigation has identified some important learning points not only for Google, but also for all organisations operating online, particularly when they seek to combine and use data across services. It is vital that there is clear and effective information available to enable users to understand the implications of their data being combined."[34]

Google amended its Privacy Policy in December 2014 and February 2015.

8.88. Yet concerns remain: in 2014 Facebook altered information posted on users' home pages, and found it could make people feel more positive or negative through a

---

26 V. Mayer-Schonberger and K. Cukier, *Big Data: A Revolution that will transform how we live, work and think*, 2013.

27 *Responsible Use of Data*, HC 245 (November 2014), para 40.

28 *Ibid*. para 41.

29 *Ibid*. para 44.

30 *Ibid.* para 45. Researchers at the University of Nottingham found that Google's 2013 terms and conditions were more difficult to understand than both Beowulf and War and Peace. Researchers used a browser plug-in called Literatin to carry out the comparison. See "Google's terms and conditions are less readable than Beowulf", The Conversation website, 17 October 2013.

31 *Ibid.* p.3.

32 Letter from the Article 29 Data Protection Working Party to Google on Google Privacy Policy and List of Possible Compliance Methods, 23 September 2014.

33 B. Van Alsenoy and others, "From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms", Draft 31/3/15, p.14.

34 See the press release on the ICO website: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/01/google-to-change-privacy-policy-after-ico-investigation/.

process of "*emotional contagion*". The study said altering the news feeds was "*consistent with Facebook's data use policy, to which all users agree prior to creating a Facebook account, constituting informed consent for this research".*[35] This generated significant media debate.

Opting out

8.89. Opting out of tracking can be a complicated process. For example:

(a) In order to opt out of Facebook's Custom Audience programme a user needs to opt out on each of the websites of the data brokers. If Facebook partners with a new data broker, the same process must be followed.

(b) Apple's Safari Browser is set to block third party cookies: yet Google was still able to send a third party cookie which operated to allow the DoubleClick cookie to be sent to the user's browser for part of 2011 and 2012.[36]

(c) Some users have found it very difficult to opt out of header enrichment.[37]

(d) Running adware/spyware removal tools may only be partially effective.

8.90. More fundamentally, our reliance on the internet, and the near-universal use of intrusive techniques, make it almost impossible to withhold consent to them. As it was recently put:

> "It's not reasonable to tell people that if they don't like the data collection, they shouldn't email, shop online, use Facebook or have a cell phone. I can't imagine students getting through school anymore without Internet search or Wikipedia, much less finding a job afterwards. These are the tools of modern life."[38]

So one can opt out of data collection, but only by opting out of 21st century society.

Anonymisation

8.91. Private companies are permitted to provide data to third parties without consent as long as the data does not contain personal data, that is, information which allows an individual to be identified. They seek to comply by providing anonymised data sets. There are increasing concerns however about the effectiveness of anonymisation techniques. A study of a number of these techniques in 2014 concluded that each failed to "*meet with certainty the criteria of effective anonymisation*".[39]

8.92. In addition, there are concerns that Big Data techniques renders anonymisation ineffective as a privacy tool: "*Given enough data, perfect anonymisation is impossible*

35 "Facebook reveals news feed experiment to control emotions", The Guardian website, 30 June 2014.
36 *Vidal-Hall v Google* [2015] EWCA Civ 311, para 3.
37 "Somebody's Already Using Verizon's ID to Track Users", ProPublica website, 30 October 2014.
38 B. Schneier, *Data and Goliath,* 2015, chapter 4.
39 Article 29 Data Protection Working Party, *Opinion 5/2014 on Anonymisation Techniques* (April 2014). The ICO published a Code of Practice on Anonymisation in 2012 which provides advice on good practice.

no matter how hard one tries".[40] In 2008, Netflix released 100 million rental records after removing personal identifiers, as part of an attempt to improve its film recommendation system. Researchers were able to de-anonymise users by comparing rankings and time stamps with public rankings and time stamps in the Internet Movie Database.[41]

The general picture

8.93. In the words of two commentators:

> "The problem is that our ability to reveal patterns and new knowledge from previously unexamined troves of data is moving faster than our current legal and ethical guidelines can manage. We can now do things that were impossible a few years ago, and we've driven off the existing ethical and legal maps. If we fail to preserve the values we care about in our new digital society, then our big data capabilities risk abandoning these values for the sake of innovation and expediency." [42]

They argue elsewhere that "*privacy protections focused on personally identifying information are not enough when secondary uses of big data can reverse engineer past, present and even future breaches of privacy, confidentiality and identity*."[43]

8.94. The issue was addressed in John Podesta's review of the implications of Big Data for President Obama in 2014:[44]

> "It will be especially important to re-examine the traditional notice and consent framework that focuses on obtaining user permission prior to collecting data. While notice and consent remains fundamental in many contexts, it is now necessary to examine whether a greater focus on how data is used and reused would be a more productive basis for managing privacy rights in a big data environment. It may be that creating mechanisms for individuals to participate in the use and distribution of his or her information after it is collected is actually a better and more empowering way to allow people to access the benefits that derive from their information. Privacy protections must also evolve in a way that accommodates the social good that can come of big data use."

8.95. The ICO published a paper in 2014 exploring the implications of Big Data for personal privacy.[45] It advised organisations to carry out robust risk assessments regarding the chance of re-identification, in light of the range of data sets available and the power of Big Data analytics.

8.96. Undoubtedly the knowledge about individuals that is available to companies and that is traded amongst them is considerable and largely invisible to the individuals

40 V. Mayer-Schonberger and K. Cukier, *Big Data: A Revolution that will transform how we live, work and think*, 2013.
41 B. Schneier, *Data and Goliath*, 2015, chapter 3.
42 J. King and N. Richards, "What's Up with Big Data?", Forbes, 28 March 2014.
43 N. Richards and J. King, "Big Data Ethics", Wake Forest Law Review, 2014, p.393.
44 Executive Office of the President, *Big data: Seizing Opportunities, Preserving Values*, (May 2014).
45 *Big Data and data protection*, (July 2014).

themselves. There are justified concerns that the consent given to data-sharing is poorly informed; that the choice given to the customer is limited or unreal; that our desire to use the services freely offered, or to obtain the benefits gained in exchange for our information, is exploited in ways that we cannot necessarily envisage; and that anonymised data, when analysed, can reveal the identity of individuals with a very high degree of certainty.

Commercial use of web logs and location data

8.97. The debate surrounding the collection of communications data centres around web logs/urls and location data. It is useful to compare how these categories of data are treated by private companies.

IP address/location data

8.98. Privacy policies often state that the use of websites may convey information about location. This can be seen in Google's privacy policy, which makes clear that Google may use IP addresses, mobile devices, search queries and information from other websites to determine location;[46] Facebook's Data Policy, which uses "*device locations, including specific geographic locations, such as through GPS, Bluetooth or WiFi"* and IP addresses;[47] and Amazon, which automatically collects and analyses IP addresses.[48] When use is made of Twitter services, Twitter may receive "*log data*" which includes the user's IP address and location. Twitter will either remove or delete the full IP address after 18 months.[49]

Web logs/urls

8.99. Google records page requests made, including the requested url;[50] and Facebook makes clear that it collects information "*when you visit third party sites and apps that use our services* (*like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit*".[51] Amazon collects and analyses the full url.[52] Using Twitter services may mean details of web pages are received by Twitter.

46 See its Privacy & Terms website: https://www.google.com/policies/technologies/ads/.
47 See: https://www.facebook.com/full_data_use_policy.
48 According to its website, see: http://www.amazon.co.uk/gp/help/customer/display.html?nodeId=502584#GUID-76787A77-872C-4019-8BD7-03C8AC3812EB__SECTION_22160257376047E78334D565CD73852D.
49 See Twitter's Privacy Policy: https://twitter.com/privacy?lang=en
50 See https://www.google.com/intl/en/policies/privacy/key-terms/#toc-terms-server-logs.
51 See https://www.facebook.com/policy.php.
52 As explained at: http://www.amazon.co.uk/gp/help/customer/display.html?nodeId=502584#GUID-76787A77-872C-4019-8BD7-03C8AC3812EB__SECTION_22160257376047E78334D565CD73852D.

Visits to websites with social plug-ins

8.100. The use of plug-ins (8.81 above) automatically sends information to companies such as Facebook, Google and Twitter.[53] Research published in March 2015 claimed that:[54]

(a) Facebook sets a cookie on certain non-Facebook pages enabling tracking by social plug-ins even if a user never visits a Facebook page. Information transmitted as a result of cookies can include an IP address, according to Facebook's Data Policy.[55]

(b) When a logged-in Facebook user visits a site with a Facebook social plug Facebook receives the url of the web page being visited.

(c) When a user logs out of Facebook, Facebook keeps uniquely identifying cookies in the browser which are used to track these users across the web using social plug-ins.

(d) When a Facebook user deactivates an account, Facebook does not remove certain cookies which are used to track these deactivated users across the web using social plug-ins.

Public use of commercial data

8.101. The information given to private sector companies is relevant not only as a comparator, but as a direct contributor – or potential contributor – to law enforcement. As the Director of Europol has claimed:

> "We know much less than the private sector. All recent cyber crime operations you've heard about on the news were launched on the basis of information provided by the private sector."[56]

8.102. Two examples are as follows:

(a) It was reported in 2005 that the FBI was purchasing data from a data broker to help keep track of suspected terrorists. This led to concerns that limitations placed on government to carry out surveillance were being avoided by the use of private companies.[57]

(b) It is claimed that the Snowden Documents show that the NSA used Google's Doubleclick service to identify Tor users. GCHQ and the NSA were said to use

---

53 Pressing the button is not needed: visiting the web page is sufficient in all three cases.

54 G. Acar, B. Van Alsenoy, F. Piessons, C. Diaz, B. Preneel, "Facebook Tracking through Social Plug-ins", March 2015, https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf. Facebook states that this report and/or earlier drafts contain factual inaccuracies: "Facebook hits back at data usage privacy criticisms", BBC News, 1 April 2015.

55 See https://www.facebook.com/help/cookies/.

56 R. Wainwright, "Cybercrime and the challenges for law enforcement", speech to LIBE Committee, European Parliament, 11 November 2014.

57 "FBI, Pentagon pay for access to trove of public records", Government Executive website, 11 November 2005.

this information to "*enable remote exploitation*". It was also said that NSA gathered location data from apps to track devices.[58] These examples have led to the claim that "*government surveillance piggybacks on corporate capabilities*."[59]

8.103. This all emphasises the need for independent supervision of the use of bulk datasets, as has taken place for several years (though such supervision has only recently been avowed).[60]

Relevance of private sector activity

8.104. The conduct of private companies cannot excuse the state from protecting the rights of its citizens, however excessive that conduct may seem to some. As an industry voice reminded me: "*The state can arrest you or lock you up ... the worst Google can do is show you an ad".*[61] Safeguards on the exercise of intrusive powers are, for that reason, more important where the state is concerned. Private companies have not been slow to seek constraints on the authority of states to exercise their powers.[62]

8.105. But in relation to capabilities, a different logic applies. Companies aim to make profits (and may do so by enhancing the convenience of their customers). The state exists for the more fundamental purpose of protecting its citizens from threats to their lives and security. Its need for intrusive powers could thus be characterised as more pressing. Furthermore, in the UK at least, substantially more people express concern about the monitoring of their online activity by social media websites and search engines than about the activities of either the US or the UK Government: 2.27(a) above.

8.106. Thus:

(a) It may legitimately be asked, if activity of a particular kind is widespread in the private sector, why it should not also be permitted (subject to proper supervision) to public authorities.

(b) The extent to which we think it normal to share personal information with private sector providers will in any event tend to condition the terms in which we think about what it is acceptable to allow the state to do on our behalf.

---

58 "NSA uses Google Cookies to pinpoint targets for hacking", The Washington Post, 10 December 2013. The issue of whether it is fair to conflate private companies' activities with government surveillance is discussed in the article. One contributor noted "*There's increasingly a sense that giving consumers control over the information they share with companies is all the more important because you're giving them control over the information they share with government.*"

59 *Data and Goliath,* 2015, chapter 6.

60 7.69 and 8.26-8.29 above; Recommendations 81(b) and 91(d) below.

61 The requirement of consent for private sector intrusion is another distinguishing factor, though its practical value may be doubted: 8.84-8.96 above.

62 The campaign for Global Government Surveillance Reform, supported by a number of large private companies including Google and Facebook, promotes as its first principle: "*Limit governments' authority to collect users' information*."

PART III: PERSPECTIVES AND VISIONS

Part III of the Report (PERSPECTIVES AND VISIONS) draws on the submissions and evidence received by the Review in order to summarise the wishes of interested parties.

- **Chapter 9 (LAW ENFORCEMENT)** summarises the requirements of the NCA, police, local authorities and other law enforcement bodies. It addresses the utility of interception and communications data for their work and their views on capabilities and safeguards.

- **Chapter 10 (INTELLIGENCE)** summarises the submissions made to the Review by the security and intelligence agencies: MI5, MI6 and GCHQ. It explains their views on technological change and encryption, what they say they need to maintain existing access, and their priorities in relation to capabilities and authorisation of warrants.

- **Chapter 11 (SERVICE PROVIDERS)** summarises the submissions made to the Review by communications service providers, both in the US (regarding cooperation with the UK Government and extraterritorial effect) and in the UK (where there was a strong emphasis on the strengthening of controls and oversight).

- **Chapter 12 (CIVIL SOCIETY)** summarises the case made to the Review by civil society groups and individuals, some of whom challenged the need for current capabilities and most of whom emphasised what they saw as the need for transparency, coherence, clarity and improved scrutiny and safeguards.

9. LAW ENFORCEMENT

Scope and sources

9.1. This Chapter seeks to summarise the views expressed to me by users of intercepted material and communications data (other than the security and intelligence agencies, which are covered separately in Chapter 10).

9.2. Leaving aside the security and intelligence agencies, the 600 or so public authorities with the power to request ***communications data*** comprise:

(a) the NCA, police forces and other law enforcement agencies, which make the great majority of requests for communications data;[1]

(b) some 430 local authorities, which have their own responsibilities for enforcing e.g. trading standards; and

(c) other public authorities, ranging from bodies with enforcement powers (e.g. Charity Commission, Gambling Commission, Ofcom, Financial Conduct Authority, Medicines and Healthcare Products Regulatory Agency, Health and Safety Executive) to the Maritime Coastguard Agency, an occasional user of communications data in the context of saving lives at sea.

9.3. I refer to these bodies collectively as "*law enforcement*", though some of them make use of their powers for other purposes. The bodies at 9.2(b) and (c) above are referred to as "*the minor users*", since they are currently responsible between them for only a little over 1% of all communications data requests.

9.4. Of those public authorities, once again leaving aside the security and intelligence agencies, five (the NCA, MPS, PSNI, Police Scotland and HMRC) also have the power to ***intercept*** communications under RIPA Part I Chapter 1. 2,795 interception warrants (and a far greater number of modifications) were approved in 2014, including on application by the security and intelligence agencies: 68% concerned serious crime and 31% were on grounds of national security.[2]

9.5. I received written submissions from each of the intercepting authorities (sometimes, as in the case of the MPS, NCA and Police Scotland, more than once) and from ACPO, the LGA and a number of public authorities with communications data powers. Most of those submissions are confidential, but where I have permission to publish them I have done so[3] I also visited and/or spoke to many other organisations;[4] and the Communications Data Strategy Group (which blends UK CSPs and law

1 In 2014, they were responsible for 88.9% of authorisations and notices under RIPA Part I Chapter II, as against 9.8% for the intelligence agencies, 0.4% for local authorities and 0.9% for other public authorities: *IOCC Report*, (March 2015), Figure 7.

2 *Ibid.*, Figure 2. The national security warrants however include the 20 s8(4) "*bulk*" warrants.

3 Ofcom (permission granted 2 April) and the ACPO (permission granted 24 April)

4 The Home Office, the NCA, the Metropolitan Police Commissioner, the MPS Assistant Commissioner for Specialist Crime and Operations, the Chief Constable of the PSNI, the National Policing Lead for Communications Data, the MPS Communications Intelligence Unit **[CIU]**, MPS SO15 Communications Data Team (on behalf of police National Counter-Terrorism), Data Communications Group Futures, Gloucestershire Constabulary, Nottinghamshire Police, the LGA and NAFN.

enforcement) and the police Data Communications Group executive committee held special meetings which enabled me to quiz them extensively on their priorities.

9.6. There has been no attempt to formulate uniform views within the law enforcement community, or to put such views across to me. Rather, I set out here ideas from a variety of sources, some of which I draw on in my recommendations (Part IV, below).

Summary of requirements

9.7. In essence, and subject to the widely understood requirements of necessity and proportionality, law enforcement bodies want the ability to access the communications data (or, in serious cases, intercept the communications) of anybody within the UK who may be involved in crime or a threat to public safety, whether as suspect, victim, or witness. When dealing with vulnerable and missing persons, they require the same ability in order to save life and protect people from significant harm.

Digital policing

9.8. The principle of policing by consent[5] is applied by the police to the digital world, where it refers to the use of techniques that command general acceptance. I was told that just as the public would not accept the existence of physical no-go zones in towns and cities, so they expect the police to have the capacity, in appropriate cases and when duly authorised, to trace any kind of communication.

Capabilities

9.9. Law enforcement strongly supports a continuation of data retention by CSPs, as now provided for under DRIPA 2014, accepting 12 months routine retention as a proportionate level.

9.10. It is also considered important to have a fully effective means of IP address resolution. CTSA 2015 is regarded as a useful stepping-stone in that regard. But it does not fully enable IP address resolution, in particular dynamic IP resolution,[6] which requires more data to be retained by service providers, depending on their individual technical model. If that resolution could be achieved by service providers retaining this additional data, including for many service providers the destination IP address, law enforcement would support such a requirement.

9.11. The Communications Data Bill contained provision for the retention of third-party data and for a request filter. Law enforcement still endorse the operational requirements which those provisions were meant to address, but want to engage further with industry on the best ways of meeting them.

9.12. The NCA indicated to me a number of other powers that they think should be considered, including (on a US model) powers to access data flow analysis and to

---

5 This is a reference to the time-honoured principle, attributed to Sir Robert Peel and contained in the General Instructions issued to new police officers since 1829, that the power of the police "*is dependent on public approval of their existence, actions and behaviour and on their ability to secure and maintain public respect*".

6 See 4.18 above.

obtain the pre-emptive seizure of intangible property such as IP addresses and domain names; and a clear enumeration of powers relating to non-notification of subjects and the possible future use by law enforcement of CNE.

9.13. Some users not currently entitled to it (DWP, and teams within certain local authorities) would like to see the extension of their powers to cover traffic data where that would enable them more effectively to tackle the crimes for which they have investigative responsibility. This was not, however, the position of the LGA when we spoke to its representatives.

Authorisation and review

9.14. There is unanimous support for the SPoC arrangements and (among local authorities) for the centralisation of those arrangements into NAFN, which some thought could be further extended. There was markedly less enthusiasm for the recently-introduced requirement of authorisation by magistrate for communications data requests, which has also been criticised by IOCCO and the OSC.

9.15. IOCCO is widely praised for its increasingly effective monitoring and for its constructive approach. I received no comments from law enforcement about the systems for parliamentary control or judicial oversight.

Utility of intercept and communications data

No intercept as evidence

9.16. The product of UK lawful intercept is only available as an intelligence tool: with limited exceptions, it is not admissible as evidence. Though foreign interlocutors often find it hard to credit, this limitation has survived repeated scrutiny. Part of the reason for this is the extensive disclosure requirement in criminal proceedings: were it sought to rely on the product of intercept conducted over a period of several months, the defence could legitimately request a transcript of the entire intercept product with a view to searching it for exculpatory material. As the latest review put it, unless budgets were increased:

> "the increased resource burden would mean either that a very large amount of other agency activity was dropped to fund intercept as evidence or that interception would be available for many fewer investigations – or both."[7]

9.17. That extensive review, overseen by a cross-party group of Privy Counsellors under Sir John Chilcott, led to the Government confirming that there should be no change (at least for now) to the current position. The Security Minister stated that "*[t]he costs of translation, transcription and retention in order to disclose material to the defence would be substantial, diverting considerable resources away from investigative work*", that "*the benefits – measured in additional convictions – would be highly uncertain*" and that "*the costs and risks of introducing intercept as evidence are disproportionate*

7 *Intercept as Evidence* Cm 8989, (December 2014).

to the assessed benefits".[8] That statement echoed the conclusions of seven previous reviews since 1993, and is accepted by law enforcement.

9.18. This important limitation (which it is not within my remit to revisit) places a premium on obtaining content by other means: e.g. by interrogating devices and by applications to a court for stored communications. The content of communications taken from a computer or phone may be and commonly is deployed in evidence, as indeed foreign intercept may be. The Crown Prosecution Service **[CPS]** point out that the bar on the use of intercepted material places further emphasis on the use of communications data to secure convictions.[9]

Utility of interception

9.19. The relative impact of interception is probably in decline, as communications data become more abundant, criminals become more security-aware and communications migrate to internet-based apps, managed by providers in other countries in which interception by UK authorities may not be a realistic option. Interception is therefore used only in the most serious cases. I return to the subject of authorisation at 9.90 below.

9.20. But interception can still be of vital importance for intelligence, for disruption, and for the detection and investigation of crime. Some examples are given at Annex 8 to this Report. Interception warrants are issued to assist in dealing with serious crime at an average rate of about five a day. The lead in developing and maintaining interception capability is with NTAC, part of GCHQ, with whose concerns I deal in Chapter 10 below.

Utility of communications data

9.21. The great majority of communications data use is for the prevention or detection of crime, or the prevention of disorder.[10] Other than national security, the next most used statutory purpose is the emergency prevention of death or injury, for example in the case of a kidnap or missing person.

9.22. The significance of messaging and social media in terrorism prosecutions is immense. The CPS reviewed a snapshot of recent prosecutions for terrorist offences and concluded that in 26 recent cases, of which 17 have concluded with a conviction, 23 could not have been pursued without communications data and in 11 cases the conviction depended on that data.[11]

9.23. Securing reliable access to communications data was also described to me as a necessary part of the fight against online crime (including child sexual exploitation and fraud) and a staple of investigations into serious and organised crime. I was told that communications data was "*an essential tool in investigating even the minor volume*

8 *Intercept as Evidence: Written Statement* (James Brokenshire MP, 17 December 2014, HCWS124).

9 Evidence to the Review, April 2015.

10 78.5%, as against 15% for national security, 6% for the emergency prevention of death or injury and 0.5% for others (including tax, public health and investigating miscarriages of justice) *IOCC Report* (April 2014), Figure 8.

11 Evidence to the Review dated 1 October 2014.

crimes that are key indicators of police performance and public confidence".[12] Police Scotland pointed out that it "*directly affected the outcome ... establishing the whereabouts of individuals and saving lives*" in over half of all "*threat to life*" incidents in Scotland in the latest three-month period.[13]

9.24. Both in the context of this Review and in my capacity as Independent Reviewer of Terrorism Legislation, I have acquired some familiarity with the resourcefulness and knowhow that are deployed in these contexts. Communications data are frequently used in the course of fast-moving operations, in which access will often be needed to data in something close to real time. Some of this work is highly resource-intensive, and depends on very quick decision-making by highly skilled experts:

(a) An example, which I observed on a visit to the MPS' SPoC was an unfolding kidnap investigation in which requests for communications data were being made every few minutes in an effort to detect the perpetrators' movements and contacts;

(b) I was taken in detail through a five-week investigation, led by the CIU, following a report that a child had gone missing. It progressed from being a high-risk missing person investigation to kidnap, murder and ultimately a manhunt and arrest. Five SPoCs were dedicated to the investigation, day and night, throughout the five weeks. More than 30 UK service providers and several foreign law enforcement agencies were engaged, and more than 900 RIPA requests for communications data were generated in an investigation where quick reactions and flexible procedures were at a premium.

(c) The CPS has illustrated for me, by reference to 30 terrorism prosecutions, the central role that digital policing has in the investigation and prosecution of terrorism offences. The ability to extract evidence from social media and messaging relating to a security-aware individual is exemplified by the recent conviction of Imran Khawaja, a British fighter and propagandist for ISIL in Syria.[14]

(d) The NCA illustrated the importance of retained communications data to establishing who was involved in a conspiracy, helping to ensure that leading members are identified and convicted. Attique Sami was sentenced to 19 years in March 2015 for conspiracy to supply and import Class A drugs, some 238kg of heroin with a street value of £38m. Crucial to his conviction was the use of retained communications data to identify that he had organised a meeting of the co-conspirators because, although the meeting was under surveillance, his presence there had not been identified.

---

12 Submission of PSNI to the Review, November 2014.

13 Evidence of DCC Iain Livingstone, April 2015.

14 Sentencing remarks of Mr Justice Jeremy Baker in *R v Khawaja, Bhatti and Ali* at Woolwich Crown Court, 6 February 2015, accessible at https://www.judiciary.gov.uk/wp-content/uploads/2015/02/khawaja-sentencing-remarks1.pdf. Further detailed evidence prepared for me by the CPS was cleared for use too late for inclusion in this Report.

9.25. Though the use of communications data is particularly prominent in online crime such as fraud and child sexual exploitation, I have been shown examples of it also in relation to crimes in action (e.g. kidnap for ransom, blackmail), trafficking (whether of people, drugs or weapons), crimes of violence (when communications data can corroborate new information, often some time after the event), harassment and malicious communications. As the National Policing Lead for communications data put it to me: "*Cybercrime is not solely the responsibility of specialist units, but is a growing general policing challenge.*"[15]

9.26. Communications data may also be needed in order to meet public expectations that the police will be able to solve even relatively low-level crimes. Thus, where someone has their mountain bike stolen and sees it advertised for sale on an online marketplace such as Gumtree, investigators may need to apply, as a minimum, for subscriber information to pursue the case.

9.27. Where ordinary policing is concerned, and still more so in the case of many minor users, it is generally accepted that much remains to be done in ensuring that existing capabilities are used to the full. Gaps in the existing law, and the authorisation procedures required in particular of local authorities, are also said to stand in the way of a more effective response to the threat. It was noted that although the IOCC expressed the tentative view in 2014 that more than 500,000 authorisations and notices "*has the feel of being too many*",[16] his subsequent rigorous inquiry into whether there was significant institutional overuse of the powers concluded that there was not.[17]

9.28. Of central importance, I was told, was the ability to use communications data (subject to necessity and proportionality) for:

(a) linking an individual to an account or action (e.g. visiting a website, sending an email) through IP resolution;

(b) establishing a person's whereabouts, traditionally via cell site or GPRS data;

(c) establishing how suspects or victims are communicating (i.e, via which applications or services);

(d) observing online criminality (e.g. which websites are being visited for the purposes of terrorism, child sexual exploitation or purchases of firearms or illegal drugs); and

(e) exploiting data (e.g. to identify where, when and with whom or what someone was communicating, how malware or a denial of service attack was delivered, and to corroborate other evidence).

---

15 Submission of Richard Berry, National Policing Lead for Communications Data, to the Review, 29 September 2014.

16 *IOCC Report*, (April 2014), para 4.28.

17 *IOCC Report*, (March 2015), para 7.94. He did however find some examples of the powers being used improperly or unnecessarily.

9.29. These requirements have not changed substantially since 2012, when the Communications Data Bill was proposed. But I was told that law enforcement has an improved understanding of how difficult it can be to achieve them, and of the technical issues involved. It has recognised, in particular, that in order to maintain efficacy in a digital world, the approach in any new law has so far as possible to be flexible and pragmatic rather than prescriptive.

9.30. Law enforcement argues that communications data provision is much less intrusive than:

(a) other surveillance methods (such as interception, directed surveillance intrusive surveillance and the use of CHIS); and

(b) evidential powers under PACE of search, seizure and interrogation.

All of these might only result in obtaining the same level of understanding about a suspect and those involved in a crime. Use of communications data can build a case for using a more intrusive measure, or deliver the information that makes other measures unnecessary. It can, and does, exonerate innocent people without them needing to know that they were ever under suspicion. Its marginal cost is low; it can be started, changed and stopped easily; it involves a low risk of compromising an investigation by being discovered by the suspects; and it is able to be used much more widely than other forms of surveillance.

9.31. The phrase "*digital witness*" sums up the approach of law enforcement to the use of their powers. Just as it is expected practice for the police to seek the human witnesses to any event that they are investigating, so they argue that they would be failing in their duty were they not to seek the digital evidence that relates to a crime or other allegation. For example, in a recent case of serial stranger rape presented on the BBC Crimewatch programme, the crimes took place in locations where there was no CCTV and away from residential areas. A key line of enquiry was to consider CD and digital options (including traffic data) to locate the victim, potential witnesses and possible suspects.

9.32. Communications data has long been an essential part of many prosecutions: there can have been few organised crime cases in which phone logs were not adduced in order to establish a pattern of communications between conspirators. Nor, even, is the ability to trace the location from which a call was made entirely novel: fixed lines have always been in known locations. The NCA and police see their current powers as, in large part, a translation of that well-established resource into the current age. Indeed they fear its dilution, as explained below.

Capabilities: interception

9.33. The capability to intercept communications is uncontroversial. But the point was made to me by SO15, and to a lesser extent by the NCA, that current warrantry requirements were very inflexible: "*so many pieces of paper on the same target: different routes, different authorisation levels, not much flexibility of timescale*". There was support for greater use of dual warrants, or thematic warrants, or warrants more focussed on the

level of crime being investigated than on the specific technique that it was proposed to use at any given time.

Capabilities: communications data

Perception of the problem

9.34. Law enforcement view themselves as engaged in a difficult struggle with serious and organised criminals and terrorists, a struggle in which their opponents hold many of the advantages. Increasing numbers of their targets are employing techniques such as Tor, PGP and VPN to ensure their anonymity:[18] they can be hard to discover, and communications data can be an important part of the answer.

9.35. The National Policing Lead singled out IMS (see 4.16 above) as a particularly significant challenge to future capabilities. He also told me that it was becoming more difficult to attribute a device to a person, to discover the true user of an identifier, to identify the location of a device at the time of use or when trying to locate a victim, to identify which service has recorded some of the data, to separate CD and intercept material and to analyse without bulk machine-based techniques.[19]

9.36. As a senior counter-terrorism officer put it to me: "*We have had 15 years of digital coverage being the main thing – a golden period. But the way people run their lives is not so accessible to us now.*" Human surveillance and use of CHIS were not seen as effective substitutes. As the National Policing Lead emphasised, the alternatives to the use of communications data tend to be more intrusive and to carry both a higher associated cost (in equipment and workforce deployment) and a higher risk to those deployed.

9.37. No one sought to quantify for me the shortfall in information, after an ill-fated attempt to do so in 2012.[20] I was told that law enforcement only records what it can use and access, not what it cannot. But in summary, it has access to a decreasing proportion of an increasing quantity of digital information.

9.38. Some specific business, technical and legal risks were identified, including:

(a) the ***reduction in the routine retention*** of communications data by service providers for business purposes (because, for example, inclusive tariffs make it unnecessary to keep details of every call made);

(b) the ***growth in OTT services***, typically provided from outside the UK and through service providers who may be less willing or able to cooperate;

(c) difficulties in ***resolving IP addresses*** (i.e. attributing an action on the internet, including sending an email, to a particular device); and

---

18 4.46 and 4.65-4.68 above.

19 Submission to the Review of Richard Berry, National Policing Lead for Communications Data, 29 September 2014.

20 JCDCDB Report, paras 34-36.

(d) the ***Digital Rights Ireland*** judgment, which appears to place limits on the powers of EU Member States to practise data retention, and even to revive the debate over whether a data preservation model (as used in Germany, and under which data are retained only on limited categories of person) should be used instead.

Legislative solution

9.39. The policy debate is thus a particularly difficult and delicate one. Existing powers are perceived as being under technological and legal threat, just as the law enforcement case for adding to them (running, they would say, to stay still) is growing in force. But it is fair to say that whilst both police and NCA see the need for change, neither has expressed to me a clear view on the form that any new powers should take. They say that it is their role to outline operational requirements against which Parliament should consider what powers are needed.

9.40. Limited consultation leading up to the Communications Data Bill 2012, and a further two years since early 2013 in which political disagreements made it impossible to take things farther, leave an uncertain position which I attempt to describe but which can only be resolved by further intensive consultations between Government, law enforcement and service providers.

9.41. The debate concerning communications data capabilities may be organised under five overlapping heads: ***data retention, IP resolution, web logs/destination IP addresses, third party data*** and the ***search filter***. I summarise the position of law enforcement on each of these, before addressing some further capability matters that the NCA raised with me during the course of the Review.

9.42. Both police and the NCA were keen to emphasise that they want to work with industry to identify solutions that would meet their investigatory requirements in a way that could inform legislation. Those requirements are very likely to include data retention and IP resolution, but in other respects may or may not fall under the same headings as the 2012 Bill. As the MPS put it to me:

> "a less '*technology-centric'* approach may assist in ensuring flexibility and agility in meeting our future capability requirements."[21]

Data retention

9.43. Successive UK Governments have supported the compulsory retention of communications data by service providers.[22] The principle that communications data generated by service providers should be required to be retained by UK service providers for a certain period, as provided for in DRIPA 2014 s1, (and previously by the EU Data Retention Directive of 2006), passed through Parliament with few

21 Evidence to the Review, April 2015.

22 The UK was one of four Member States that put forward the original proposal for the mandatory retention of data in 2004, and used its Presidency of the EU to prioritise the draft EU Data Retention Directive in the months after the London bombings of July 2005: JCDCDB Report, para 4.

difficulties in July 2014, though with a sunset clause to require further consideration.[23] It has the strong support of law enforcement.

9.44. In 9.21-9.32 above, I explained why the police and CPS consider communications data in general to be essential for the fight against crime. The specific role of retained data in investigations into sexual offences, terrorism, drugs, homicide, firearms and explosives is explained at Annex 10 to this Report.

9.45. The police and CPS make three other points in this regard:

(a) Conspirators become more guarded in their use of communications as the moment of a crime approaches. Older data may therefore be the best evidence against them.

(b) It may be relatively easy to arrest the minor players in a drugs importation or smuggling ring. But by going through their historic communications data, it may become possible to trace the bigger players who have taken care to remain in the background.

(c) A time lapse between the incident and the identification of a suspect will mean that old data is needed.

9.46. Data retention is also seen as an imperative by law enforcement outside the UK. In a presentation to the European Parliament Committee on Civil Liberties, Justice and Home Affairs last year, the Director of Europol, said that "*without data retention law the police will not be able to catch criminals harming our society*", adding:

> *"*Ask yourself what the end of data retention would mean in concrete terms? It would mean that communication data that could have solved a murder or exonerate a suspect is simply deleted and no longer available."[24]

9.47. DG Home at the European Commission has drawn attention to the negative consequences for law enforcement in countries such as Germany and the Czech Republic where data retention has ended.[25] As the Commission noted in 2014:

> "Member States have generally reported that retained data is very valuable, and in some cases indispensable, for preventing and combating crime, for protecting victims and for the acquittal of the innocent in criminal cases.
>
> ...
>
> Data retention enables the construction of trails of evidence leading up to an offence. It also helps to discern or corroborate other forms of evidence on the activities of and links between suspects and victims. In the absence of forensic

23 The maximum period is set at 12 months under DRIPA 2014 s1(5).

24 R. Wainwright, Presentation to European Parliament Committee on Civil Liberties, Justice and Home Affairs, 11 November 2014.

25 DG Home European Commission, *Evidence for necessity of data retention in the EU*, (March 2013) which can be accessed at: http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf.

> or eye witness evidence, data retention is often the only way to start a criminal investigation. Generally, data retention appears to play a central role in criminal investigation even if it is not always possible to isolate and quantify the impact of a particular form of evidence in a given case."[26]

Even the CJEU, which invalidated the EU Data Retention Directive in April 2014, described data retained under the Directive as "*a valuable tool for criminal investigations*". The court which rendered the Dutch data retention law inoperable in March 2015 added that "*the detection of certain types of crimes rely almost exclusively on the use of historical telecommunications data*".[27]

IP resolution

9.48. In CTSA 2015 Part 3, Parliament extended the scope of compulsory data retention by service providers to include the data that are needed to link an IP address with the device that was using that address at a particular time. The issue was explained as follows in the Explanatory Notes to the Bill:

> "[IP] address resolution is the ability to identify who in the real world was using an IP address at a given point in time. An IP address is automatically allocated by a network provider to a customer's internet connection, so that communications can be routed backwards and forwards to the customer. [CSPs] may share IP addresses between multiple users. The providers generally have no business purpose for keeping a log of who used each address at a specific point in time."[28]

9.49. There was unanimous support from law enforcement for this change. The data that must now be retained are communications data that relate to an internet access service (e.g. home broadband, mobile internet or public WiFi) or an internet communications service (e.g. internet telephony, internet email, instant messaging), and that:

> "may be used to identify, or assist in identifying, which [IP] address, or other identifier, belongs to the sender or recipient of a communication (whether or not a person)".[29]

There is however an exception, which was explained as follows in the Explanatory Notes:

> "Subsection (3)(c) specifically prevents a telecommunications operator providing an internet access service from retaining under this legislation data

---

26 European Commission, "Frequently asked questions: the Data Retention Directive", (April 2014).

27 See 5.62 and 5.67, above.

28 Counter-Terrorism and Security Bill, Explanatory Notes, November 2014, para 121.

29 CTSA 2015 s21(3)(b). In the words of the Explanatory Notes of 8 January 2015: "*Such data could include data required to identify the sender or recipient of a communication (which could be a person or a device), the time or duration of a communication, the type, method or pattern of a communication (e.g. the protocol used to send an email), the telecommunications system used or the location of such a telecommunications system that the person was communicating from. An IP address can often be shared by hundreds of people at once – in order to resolve an IP address to an individual other data ("other identifier" in this clause) would be required. Data necessary for the resolution of IP addresses could include port numbers or MAC (media access control) addresses*."

> that explicitly identifies the internet communications service or websites a user of the service has accessed. This type of data is sometimes referred to as web logs."

That exception (and even its description) remains controversial, as discussed below.

9.50. The utility of the new requirement may be demonstrated by the scenario in which the police get hold of a server that was used to host criminal activity. They can retrieve the IP addresses that contacted it; but without the ability to resolve IP addresses which may have been used over time by more than one device, will not know the specific computer or phone that was using each address at the time when contact was made.

9.51. Law enforcement bodies welcome CTSA 2015 Part 3, believe that it will have some independent utility in resolving IP addresses, and want an equivalent provision to be introduced after the end of 2016. They also emphasise however that it is no more than a stepping-stone. Some CSPs, particularly, those using dynamic IP addresses such as mobile phone operators, require destination IP as well as sender IP to match up who is involved in an action. There is a strong belief that the exclusion in CTSA 2015 s21(3)(c) may need to be revisited if reliable IP resolution is to be achieved. But as explained below, this does not necessarily mean that law enforcement bodies want any more than is needed to maintain their operational capabilities.

Web logs / destination IP

9.52. The Home Office explained to the JCDCDB that it wanted law enforcement to be able to access "*two specific types of data: subscriber data relating to IP addresses and web logs*".[30] The retention of the former has been provided for by CTSA 2015 s21(3): but for the time being at least, the same Act excludes the compulsory retention of web logs (see 9.49 above).

9.53. What is meant by web log in this context has caused some uncertainty, and independent experts to whom I have spoken criticise the term, and those who use it, on the basis of imprecision (as well as the inapplicability of the term to non-web based services). But the Home Office has provided me with this definition:

> *"*Weblogs are a record of the interaction that a user of the internet has with other computers connected to the internet. This will include websites visited up to the first '/' of its [url], but not a detailed record of all web pages that a user has accessed. This record will contain times of contacts and the addresses of the other computers or services with which contact occurred.*"*[31]

9.54. Under this definition a web log would reveal that a user has visited e.g. www.google.com or www.bbc.co.uk, but not the specific page.[32] It could also of

---

30 JCDCDB Report, para 73.

31 Evidence to the Review, March 2015.

32 Even so, this is not straightforward. CSPs' networks are all built and configured differently and there are many datasets which could be used directly or indirectly to identify the services or sites accessed by a customer. The Home Office has indicated that such data could include but is not limited to:

- url addresses: Under the current accepted distinction between content and CD, www.bbc.co.uk would be communications data while www.bbc.co.uk/sport would be content; and this is set out in the

course reveal, as critics of the proposal point out, that a user has visited a pornography site, or a site for sufferers of a particular medical condition, though the Home Office tell me that it is in practice very difficult to piece together a browsing history, see further 14.23-14.38 below.

9.55. I am not aware of other European or Commonwealth countries in which service providers are compelled to retain their customers' web logs for inspection by law enforcement. I was told by law enforcement both in Canada and in the US that there would be constitutional difficulties in such a proposal. The new Australian data retention law is drafted in such a way as to ensure that "*service providers cannot be required to keep information about a subscriber's web browsing history*".[33]

9.56. The Communications Data Bill proposed the compulsory retention of web logs, but foundered on disagreements within the coalition Government on whether such a provision would intrude too far into privacy, particularly in view of the possible risk that web log data "*may be hacked into or may fall inadvertently into the wrong hands*".[34] The JCDCDB expressed no view on the policy issue, concluding that it was for Parliament to decide where to strike the balance, and urging the Home Office also to consider:

> "whether it would be technically and operationally feasible, and cost effective, to require CSPs to keep web logs only on certain types of web services where those services enable communications between individuals*".*[35]

9.57. In the meantime, and pending reconsideration of the law which is set to expire at the end of 2016, the retention of web logs has been expressly prohibited by CTSA 2015.[36]

9.58. The law enforcement bodies which spoke to me required the ability to resolve IP addresses, but some were unwilling to be prescriptive about how this could best be achieved. It was recognised that some service providers may require destination IP

Acquisition Code. However there are arbitrary elements to that definition – for example sport.bbc.co.uk (no 'www.') takes you to the same place as www.bbc.co.uk/sport.

- Destination IP address: All devices connected to the internet have an IP address. In terms of a technical hierarchy, these sit below the url address, allowing the url to function, and are also used for more than just web surfing. A log of IP addresses can tell you what websites and individual has viewed but some services (e.g. Google) are hosted on multiple IP addresses while some IP addresses may host more than one website. A log of IP addresses can also tell what communication apps/services an individual has accessed e.g. Whatsapp or Facebook Messenger. Apps and services do not generally have url addresses.
- DNS server logs: A DNS (domain name system) translates a domain within a url addresses (typed by average web browsers) into the IP addresses used by a computer to make the connection.
- http 'GET' messages: These are machine-to-machine messages that facilitate the transfer of information when viewing web pages
- IP service use data (summarised service use/category information, frequently derived from network management systems) CSPs can profile customers' web history using network management systems, for example by comparing a customer's browsing history against pre-set parameters to define the types of services they have been accessing.

33 Telecommunications (Intercept and Access) Amendment (Data Retention) Act 2015, s187A(4)(b), excludes from the retention obligation information obtained by the service provider as a result of providing the service "*that states an address to which a communication was sent on the internet, from a telecommunications device, using an internet access service provided by the service provider*".

34 JCDCDB Report, para 86.

35 *Ibid.*, para 88.

36 CTSA 2015 s21(3)(c).

addresses for the purposes of resolution, but the view was expressed that destination IP addresses are less intrusive than web logs and that service providers which do not require even destination IP addresses for the purpose of resolution should not be obliged to keep them.

9.59. Others emphasised the point that the compulsory retention of web browsing history could have advantages for law enforcement. As well as assisting in the resolution of IP addresses, it could:

(a) identify ***communications sites*** that have been used by a particular device, thus enabling further enquiries to be carried out to establish details of their communications through those sites; and

(b) more broadly still, identify sites visited which might be ***suggestive or corroborative of criminality***: for example, sites associated with terrorism, paedophilia or the sale of counterfeit goods.[37]

9.60. But it is widely accepted within the law enforcement community that:

(a) the compulsory retention of web logs would be potentially intrusive;

(b) the political environment (not to mention the legal environment: *Digital Rights Ireland*) may not be conducive to the imposition of such an extensive obligation; and that

(c) there would be expense and complexity involved in making these changes (not least in terms of training staff within law enforcement), that would only be justified if any new power were to be extensively used.

9.61. In short, it was not submitted to me, as it was in 2012 to the JCDCDB, that "*access to weblogs is essential for a wide range of investigations*".[38] IP resolution is seen as vital, both from IP addresses to individuals and vice versa; and it was clear from my conversations with the most senior officers that law enforcement does want a record to exist of an individual's interaction with the internet to which it can obtain access. Ultimately it would argue for the retention of web logs, subject to safeguards to be determined by Parliament, if this was identified as the best way to meet its operational needs. But it would expect all avenues to be explored before reaching a final view on the best solution.

Third-party data retention

9.62. The draft Communications Data Bill in 2012 provided for UK CSPs to be required to retain and disclose third-party data, i.e. communications being sent over the network of a UK CSP, where the third party would not comply with the requirement to disclose the data. This was in the expectation that some overseas service providers would not cooperate with requests from UK authorities and that therefore a back-up capability

[37] The MPS also told me, in April 2015, that web logs "*may assist in discovering on line bookings for travel (assist surveillance), interest in property purchase (asset recovery) or financial dealings (evidence of principal offence or criminal asset recovery*)": a very broad range of sites indeed.

[38] JCDCDB Report, para 85.

was needed. The Home Office gave an oral commitment to UK CSPs that "*the Home Secretary will invoke the third party provisions only after the original data holder has been approached and all other avenues have been exhausted*".[39]

9.63. UK CSPs were described by the JCDCDB as "*rightly very nervous about these provisions*",[40] and remain sceptical. The Government made a commitment that UK CSPs would not be required to store or decrypt any encrypted communications. But the routine encryption of communications has increased significantly since 2012: though it is still not universal, sophisticated encryption is used by a growing number of drug traffickers, fraudsters and child sex offenders. Given doubts as to whether valuable communications data could be retrieved from encrypted services,[41] the utility of this proposal needs to be re-assessed for a post-Snowden world, particularly in view of its high anticipated cost.[42]

9.64. Law enforcement bodies generally support the views of the UK CSPs in looking primarily for fuller cooperation from overseas service providers as a solution to the problem of combating criminals who use their services, whilst understanding that this will not always be possible and that the Government needs to stay alert to other possibilities. Law enforcement is also conscious that the proposal of third party data retention was a particularly expensive one, and that its utility will be peculiarly susceptible to technological developments. It may therefore be that this aspect of the Communications Data Bill is no longer judged to be the priority that it once was, even within the law enforcement community. I would note, finally, that once again the compulsory retention of such data is excluded in the new Australian data retention law.[43]

Request Filter

9.65. The 2012 Bill made provision for a "*request filter*", which would in effect allow a complex search of all companies' retained data to be made following a single request. This, it was said, would speed up investigations, minimise collateral intrusion and reduce error. It would also have made a devolved system in which the service providers each retain their own subscribers' data into something closer to the central database that was originally envisaged in 2008,[44] though the security advantages of locating the data in different places would still have been maintained.

9.66. A typical scenario for the use of a request filter would be where an investigator needed to establish a connection between people and events, which currently would involve asking service providers separately for the data on many individuals to establish who

---

39 *Ibid.*, para 109.

40 *Ibid*.

41 *Ibid.*, para 93.

42 Total anticipated economic costs of the Communications Data Bill over the 10 years from 2011/12 were estimated by the Government as £1.8 billion: the JCDCDB Report agreed with Microsoft that this cost was likely to "*have multiplied grotesquely*" (para 258).

43 Service providers are not required to keep "information or documents about communications that pass 'over the top' of the underlying service they provide, and that are being carried by means of other services operated by other service providers": note to Telecommunications (Intercept and Access) Amendment (Data Retention) Act 2015, s187A(4)(c).

44 The then Government planned to require communications data to be stored for a year in a single purpose-built database: see JCDCDB Report, para 5.

was involved in common. With an effective request filter, it would be necessary only to formulate a single, less intrusive search criterion (e.g., "*Find the devices that were in cell site area 1 on one date and in cell site area 2 on a different date*").[45] Only the data of those meeting the complex search criteria would be provided to the investigator.

CD Bill in general

9.67. In relation to the unenacted parts of the Communications Data Bill more generally, I am conscious that:

(a) There has (because of the political impasse) been very little consultation between Government, law enforcement and service providers for more than two years.[46]

(b) In particular, the CSPs have not been shown the text of the revised draft Bill that was prepared in early 2013; the NCA does not believe it has seen the final draft text; and I was myself refused permission to share it (or even a summary of it) with them.

(c) Technology has moved on since late 2012, as (since *Digital Rights Ireland*) has the legal position.

(d) Law enforcement itself wishes to reserve its detailed position on these proposals pending further discussions with a Government that has a political mandate to take it forward.

Other capabilities

9.68. The NCA identified to me a number of other capabilities for consideration. They did so in response to my own questioning, initially of front-line investigators. These ideas were formulated only late in the course of the Review, and it was not possible to road-test them with other interlocutors. Nonetheless, it might usefully be considered, in any reformulation of the law, whether it would be advantageous to provide for them.

9.69. ***Data flow analysis*** (via network protocols such as the Cisco Systems product, Netflow) is conducted by CSPs in order to ensure that their routers are operating properly and efficiently by the analysis, or sample analysis, of packets passing through them. That process analyses the attributes of each packet, including for example the source and destination IP addresses, and records may be retained by CSPs for a few days. They could be useful to law enforcement in a number of respects: for example in identifying the source or route of a denial of service attack, or malware.

9.70. Under US legislation governing "*pen register*" and "*trap and trace*", a company may be asked to hand over information about a user's communications (dialling, routing,

---

45 I was given the example of a "*three-scene murder*" (murder site, body deposition site and location of the burnt-out car used in the murder), in which the question could have been "*Which device was at all three sites between given dates and times*?".

46 The JCDCDB also criticised the consultation process prior to 2012: JCDCDB Report, para 56.

addressing and signalling information) in real time. The NCA believe that a similar power could be useful in the UK.

9.71. US law provides, secondly, for the ***pre-emptive seizure of intangible property***, by court order, so that control of it can be handed to law enforcement to use as if it is the owner. Seizure of an IP address or domain name being used for the purposes of crime (spreading malware, redirecting stolen data or hosting criminal forums) enables it to be redirected to a sinkhole[47] or to a web page used for public information and crime prevention or mitigation.

9.72. The only power which might permit such action under UK law, the Serious Crime Prevention Order, is seen as a severe and cumbersome order, time-consuming to obtain, which would inflict undesirable stigma on any service provider to whom it was directed.[48] I have been briefed on an international operation in which the lack of an easily-available seizure order handicapped the NCA's efforts in relation to a botnet used for bank fraud.[49] The point was also made to me that since the MLAT procedure cannot be used to request another country to take action that is not available in the UK, the NCA lacks the ability to request a sinkhole from the US.

9.73. A third concern relates to ***user notification***. An increasing number of US service providers have a policy of notifying users before they disclose any information to law enforcement, unless they are legally prevented from doing so, in order to allow the user to file an objection if so advised. The NCA has no objection in notification taking place, save in cases where it will hinder or undermine an investigation. In such cases, however, I am told that the NCA has withdrawn requests rather than facing the consequence of notification. The NCA and the police consider that it would be prudent to have specific legislative provision in place so that an order prohibiting notification could be obtained if appropriate.

9.74. Fourthly, the NCA draws attention to the ***divergent and rapidly-changing policies*** operated by overseas service providers in relation to the provision of communications data: what it describes as an "*ever-changing technical, jurisdictional and policy mish-mash*". This causes much time to be devoted to tailoring a request correctly, and risks resulting in the excessive acquisition of data, which is an "*error*" under the Code of Practice.[50] The NCA proposes that there should be an obligation on service providers operating in the UK to provide regularly-updated information on what data they will routinely provide to UK law enforcement, even if their position is that this is carried out on a voluntary basis. It is also suggested that UK legislation needs to allow more flexibility in how it refers to categories of data, including for example an allowance for the "*basic data package*" that service providers retain on their users.

9.75. Finally, the NCA raised with me the practice of ***CNE***. It considers that targeted CNE could give the whole communications picture of a subject at the early stage of an

47 Sinkholing is the redirection of traffic from its intended destination to one specified by the sinkhole owners (in this case, law enforcement).

48 Serious Crime Act 2007, ss1 and 41, Schedules 1 and 2. I am told that the only successful application to date, against a major drug trafficker, took three months to obtain.

49 A botnet is a large number of compromised computers that is used e.g. to generate spam, relay viruses or cause a network to fail.

50 Acquisition Code, para 6.17.

investigation, allowing a more targeted approach to those involved in the most serious criminality, and ensuring that those who adopt advanced encryption technologies remain within the reach of the law. For their part, the police consider that, in an increasingly cyber-enabled environment, the need for them to use CNE is inevitable.

9.76. A debate is clearly needed as to how law enforcement can best utilise CNE and what safeguards should apply.

Minor users

9.77. Local authorities are treated as the poor relations of law enforcement. They have to operate with a more elaborate authorisation procedure (after some well-publicised instances of the self-authorised use of surveillance powers in circumstances that seemed disproportionate).[51] Yet they manage large areas of responsibility, including tenancy fraud, benefit fraud and e-crime in the trading standards context, with diminished resources and fewer powers than most other public authorities.

9.78. Three issues arise in relation to the local authorities and the other minor users of RIPA communications data powers (as defined at 9.3 above):

(a) Who should have the powers?

(b) What powers should they have?

(c) What about non-RIPA powers?

Who should have the powers?

9.79. Not every public authority with powers to request communications data uses those powers. Indeed IOCCO reports that:

(a) 40% of the public authorities that have powers to acquire communications data have never used their powers. These are largely district councils which will have had access to non-RIPA powers for their benefit fraud functions that are now transferring to DWP; and that

(b) of the 13 public authorities which had their powers removed in February 2015,[52] only four had never used them and the remaining nine had collectively approved 103 applications for communications data in 2014.[53]

9.80. The minor users from which I have heard all wish to maintain their powers. In common with the police, they find that only the use of communications data allows them to identify subjects in some cases:

---

51 Directed surveillance, in particular, appears to have been used in relation to dog fouling, school catchment areas and the misuse of a disabled parking badge: "Spy law 'used in dog fouling war", BBC News website, 27 April 2008. Both the Conservative and Liberal Democrat manifestos in 2010 contained commitments to curb councils' powers.

52 SI 2015/228.

53 *IOCC Report*, (March 2015), para 7.10.

(a) A mobile phone number may be all that is known of someone engaged in fly tipping.

(b) Betting fraud is often conducted online and can only be tackled through an investigation online.

(c) Identifying a criminal gang planning to rob the mail is as dependent on communications data as any other investigation into a conspiracy.

What powers should they have?

9.81. Traffic data are not available to local authorities or to eight other users of communications data.[54] It was suggested to us that there is a case for according local authorities the power to request traffic data, now that a strong control regime is in place through NAFN. The same might be considered for the other eight users, were they also to use NAFN or a similar centralised, expert SPoC service.

9.82. The makings of such a case are certainly there, at least in the case of some minor users. Without traffic data, it is not possible for local authority investigators to get information about incoming phone calls, the location of phone calls and some internet use. DWP emphasised the value that traffic data would have to benefit fraud investigators, which is increasingly internet-based, not least because of Government policy to make benefits payments digitally-enabled.[55] Trading standards officers drew particular attention to the use of social networking sites, especially Facebook, being used for the sale of counterfeit goods on both large and small scale and the need for traffic data to trace the illegal action to the perpetrator.

9.83. Examples of the benefits which it is said traffic data would bring to local authority investigations are at Annex 16 to this Report. In particular it would assist in being able to secure convictions in respect of victims who are so vulnerable (primarily due to age and mental health issues) that they are not able to stand up to the rigours of the criminal justice system; and it could assist in identifying other victims, the fact of a conspiracy, the identities of conspirators and the links between suspects.

9.84. DWP indicated that it wanted power to request traffic data. Although some local authority investigators were of the same view, the LGA declined to make the same indication to the Review.

Non-RIPA powers

9.85. RIPA is not the only statute under which public authorities may obtain communications data, (see 6.16-6.18). In the recently approved Retention Code, the Government repeated its policy that communications data should not be obtained under general information gathering powers and added that retained data should only be obtained

54 These are: Health and Safety Executive, Medicines & Healthcare Products Regulatory Agency, DWP – Child Maintenance Group, Health & Social Care Business Services Organisation - Central Services Agency (Northern Ireland), Office of Fair Trading / CMA, NHS Protect, NHS Scotland Counter Fraud Services, and Department of Enterprise, Trade and Investment (Northern Ireland).

55 Evidence to the Home Office, February 2013.

under RIPA.[56] However authorities with their own powers to obtain communications data generally want to continue to use them.

9.86. Ofcom told me for example that it is able to obtain data under the Communications Act 2003, and does so frequently as part of the regulatory function. It conducted over 2,700 investigations over the past three years, often obtaining communications data to ensure that companies were behaving properly. As it said:

> *"*The information is obtained and used to protect consumers' interests. To the extent it involves data about individual consumers, their identities and conduct are incidental to, rather than under, investigation."[57]

9.87. Ofcom issued only 121 authorisations and notices for communications data under RIPA in the same period, mainly when investigating criminal offences under the WTA 2006.

9.88. The powers available to authorities under their own legislation are not overseen by IOCCO and are typically able to be authorised at a lower level within the requesting organisation. For example, executive officers in the DWP authorised to do so can obtain subscriber and service use information without further approval.

9.89. Moving to a RIPA-type approval system would have consequences for organisations now using their own powers, which will need to be thought through. There would be additional costs. The DWP in 2013 estimated their additional costs to be in the region of £1 million over three years.[58] There is a risk of anomaly in imposing the RIPA arrangement for the relatively low level of intrusion involved in a subscriber look-up, if more intrusive powers affecting individuals or businesses are not subject to external oversight. For example, Ofcom has interception powers under the WTA 2006, which it uses on a day-to-day basis to identify sources of interference to the spectrum.[59]

Authorisation of interception

9.90. Those entitled to apply for interception warrants were in general more concerned with the speediness and flexibility of the procedure than with the question of who the authorising individual should be.

9.91. Police Scotland expressed their satisfaction with the current arrangements. But others within law enforcement expressed their criticisms:

(a) A very senior police officer expressed the view that judicial authorisation would be strongly preferable to the current system of political authorisation, because of the need to have visibly robust safeguards and in order to counter any future suggestion that a warrant might have been issued for political reasons.

---

56 Retention Code, para 8.1. Retained data may also be obtained under a judicial authorisation.
57 Evidence to the Review, March 2015.
58 Evidence to the Home Office, February 2013.
59 Evidence to the Review, March 2015.

(b) The NCA made the practical point that obtaining dates for signings by the Home Secretary could sometimes be difficult, particularly where renewals are concerned.[60]

The NCA did add, however, that the current system has the desirable result of the Home Secretary "*seeing the detail of how serious crime looks on the street*". It also pointed out the need for absolute security in the arrangements for the consideration of warrants.

9.92. The NCA made a strong pitch for extending serious crime warrants to six months (in keeping with national security warrants), pointing out that a renewal application may need to be prepared before it is clear what is going on (and that the application may thus be of lower quality). A similar point was made by IOCCO in 2014,[61] and echoed by others.

Authorisation of communications data requests

SPoCs

9.93. As to the authorisation of communications data requests, the police took a good deal of pride in the SPoC system, which was said to be "*the envy of many friendly countries*". SPoCs to whom I spoke both in London and in Gloucestershire provided independent input into the process in a motivated and conscientious manner, amply bearing out the IOCC's recent comment that "*the SPoC process is a stringent safeguard*".[62] SPoCs' knowledge of communications data, their relationships with service providers and their role and impact within the investigating body are crucial to obtaining the best effect from the use of the technique, and also for ensuring that it is used with least collateral intrusion. Only SPoCs are allowed to approach service providers for communications data using RIPA powers.

9.94. Within law enforcement generally, it was felt that SPoCs should have strong relationships with the investigators and this was more likely to happen where they were part of the same organisation, working to the same goal (albeit with distinct and independent responsibilities). Their effectiveness as a "*guardian and gatekeeper*" could however diminish were they to become simply part the investigation team.

NAFN

9.95. I did not detect any dissatisfaction on the part of local authorities with the role of NAFN, which (confirming the impression derived from my own visit) was praised for its proactive advice, invaluable expertise, willingness to give feedback and efficient electronic communications. Its charging system, based on a fee per organisation and a usage element, was perceived as fair. There was widespread acceptance of the view that some minor users, whose technical skills are intermittently used and not

60 Other commitments can mean that changes are made to dates that impact on whether it is possible to renew the warrant at the three-month mark, meaning that a renewal is brought forward to comply with legislation.

61 *IOCC Report*, (April 2014), para 3.44.

62 *IOCC Report*, (March 2015), para 7.46. The IOCC added at 7.47 that "*approximately 20% of applications are returned to the applicants by the SPoC for development or improvement*."

always up to date, would benefit from having their requests routed through NAFN in the same way as the local authorities do.

DPs

9.96. I received representations from the LGA regarding the status of the DP.[63] There were difficulties in determining who was entitled to act as a DP, particularly in view of what was seen as contradictory guidance from IOCCO and the OSC, and in the context of increasingly flat management structures. The LGA suggested to me that, rather than specifying the level of role required to be a DP, the requirement should be designed in terms of competency or function, with councils given the freedom to delegate the role appropriately. This is because they do not all have the numbers of staff at senior levels with ability to maintain the knowledge that is needed sufficiently to scrutinise what are only occasional applications.

9.97. Alternatively, the LGA said there may be scope to externalise or join up the DP role across councils, by appointing regional DPs, which would bring benefits in terms of training and consistency. I did not detect amongst law-enforcement personnel to whom I spoke any principled objection to authorisation for communications data access coming from outside their investigating bodies. Their main concern was that authorisation should be timely and the process as unbureaucratic as possible.

Court approval

9.98. Much less appreciated is the requirement, which is imposed only on local authorities, to have requests for communications data judicially approved by a magistrate or (in Scotland) a sheriff.[64] The LGA has not asked for its removal, though it admits to concerns about its efficiency.

9.99. Otherwise, with the exception of the Magistrates' Association, which considered that judicial approval "*ensures greater consistency of decision-making*" and "*provides greater confidence in the legitimacy and fairness of the process*",[65] few people thought that the system added value. In particular:

(a) It is described, with some reason, as extremely cumbersome: Files must go:

- from the requesting local authority to NAFN;
- from NAFN back to the local authority for DP approval;
- then from the local authority back to NAFN for the preparation of a court pack;
- from NAFN back to local authority for them to obtain court approval;

63 Evidence to the Review dated 9 March 2015.
64 See 7.56-7.61.
65 Submission of 12 March 2015 to the Review.

- to the local Magistrates' or Sheriffs' Court and back again;
- from the local authority to NAFN once again; and
- from NAFN to the service provider.

To make matters worse, whilst local authorities and NAFN communicate electronically, anything involving the court needs to be produced and transmitted on paper.

(b) It was said typically to take one to two weeks to get an appointment at the magistrates' court, and I was told of a six week delay in one case.

(c) A local authority employee may then have to spend a morning travelling to the Magistrates' Court, waiting for the case to come on, having the application approved and then returning to the office. I was told that yet further expense is incurred in Scotland, where a £90 court fee is payable and the case must be presented to the Sheriff by a lawyer.

(d) The expenditure of time and resources is said to be disproportionate to the very basic nature of most requests, particularly given that the magistrates hearing the case have no specialist knowledge and that nearly all requests are granted. NAFN told me in March 2015 that magistrates had refused only six applications since November 2012, amounting to 19 data requests, out of some 6000 requests considered by them.[66]

9.100. At the same time the number of applications from local authorities has reduced significantly. In a typical month in 2014 there were fewer than 150 requests, as against 200-400 in the months prior to November 2012: see Annex 14 to this Report. I am informed that this sudden fall in numbers, which shows no sign of being reversed, reflects of the burden on local authority investigators (particularly in time) imposed by the need to approach magistrates. That would be no bad thing if local authorities were able to do just as well with OSINT, or by consulting the Home Office's "*consented*" database of phone numbers. But I do not consider this to be the principal cause. Having spoken to a number of local authority trading standards experts, my impression is that communications data is not uniformly used as much as it could usefully be, and that the cost and delay inherent in obtaining the permission of a magistrate functions as a deterrent to applications that could properly and fruitfully be made.

Oversight

9.101. IOCCO was universally respected as a rigorous oversight body which was also beneficial in improving practices. Thus:

(a) The MPS CIU saw IOCCO as constructively critical in its approach, and would from time to time take the opportunity to ask the Commissioner's opinion about

66 Evidence to the Review from NAFN, 31 March 2015.

a proposed course of action. The staff were described as knowledgeable and increasingly technically capable, and IOCCO's recommendations as sensible.

(b) Gloucestershire Police reported to us that in the previous year they had had three visits from IOCCO of five, five and four days respectively.

(c) The NCA spoke highly of IOCCO, as did the LGA.

9.102. A number of voices however drew my attention to problems caused by the supervision of two Commissioners' offices: IOCCO for RIPA Part I and the OSC for RIPA Part II. In particular:

(a) The NCA, the LGA and IOCCO all made the point that the distinct responsibilities of the two offices meant that they lacked what was described as "*total oversight of the proportionality of the intrusion*". It may be hard, in other words, to judge whether a RIPA Part I request is proportionate (in the sense of being the less restrictive alternative), without detailed background knowledge of the directed and intrusive surveillance, CHIS etc. which may have been devoted to the same operation and which falls under the jurisdiction of a different Commissioner.

(b) I was also told, again by both the NCA and the LGA, that there are differences of approach between the different Commissioners' offices. In particular, different approaches are said to have been taken to the relative intrusiveness of different methods of surveillance, and to the identification of appropriate DPs in organisations such as local authorities in which there are no clear-cut ranks as in the police. It was not always clear whether such discrepancies were attributable to individual inspectors or to the policies of the two offices more generally.

10. INTELLIGENCE

Scope and sources

10.1. This Chapter seeks to summarise what the security and intelligence agencies (MI5, MI6 and GCHQ: referred to in this Chapter as the Agencies) - have submitted to me about the future shape of the law. It is shorter than the previous Chapter because:

(a) The Agencies, though certainly among the most important users of the relevant powers, comprise only three of the approximately 600 bodies entitled to use them.

(b) Issues relating to the Agencies' use of their powers were very recently explored, to the extent deemed compatible with the requirements of national security, in a full and careful report of the ISC.[1]

(c) For the most part, the Agencies are concerned to preserve their current powers rather than to acquire new ones.

Contact with the Agencies

10.2. My work since 2011 as Independent Reviewer of Terrorism Legislation has been chiefly concerned with the activities of Ministers, civil servants, police and prosecutors, and with the experience of those affected by the terrorism laws. Though I visit and speak regularly to all three Agencies (in particular MI5) in the context of that work, I have not in the past been exposed to the detail of their operations in the same way as the Commissioners or indeed the ISC. But in the past six months, I have acquired a degree of knowledge of the workings of the Agencies, and of their cultures, which is highly unusual for any outsider.

10.3. This Review confronted the Agencies with severe risks as well as opportunities. Nevertheless, they have engaged with me in a manner which I have found to be both open and constructive. Everything they said to the ISC, orally or in writing, was disclosed to me without question or reservation. The details of extremely sensitive capabilities have been volunteered to me, without any visible reticence. I addressed a large number of questions to the Agencies, including questions to GCHQ arising out of the Snowden Documents, and received full written answers which I was able to probe orally. I have benefited from a number of thoughtful written submissions on general and specific issues, from an intensive three-day visit to GCHQ in Cheltenham, from a number of conversations with Agency officials in posts abroad, from interviews with the chiefs of MI5, MI6 and GCHQ and from a series of sometimes lengthy meetings and demonstrations in London with each Agency.

10.4. There is, as one would expect, a range of views within each Agency as to the degree of public transparency that is appropriate. Organisations whose existence was an official secret just a generation ago are still learning to come to terms with a world which demands scrutiny, assurances and accountability at every turn. To an outsider,

[1] ISC Privacy and Security Report: see in particular chapters 3-5 (interception) and 6 (communications data).

extreme caution in relation to the release of information into the public domain can seem frustrating, and indeed contrary to the Agencies' own interests. Procedures which have never seen the light of day sometimes turn out to need improvement when they are exposed to it.[2]

10.5. Yet for what it is worth, my impression is of lean organisations by public sector standards, proud of their vital work, able to admit to mistakes, prizing agility and resourcefulness but accepting the need to be held to high ethical and legal standards. They seek to promote public confidence via trusted public-facing intermediaries (whether the Commissioners, the ISC or myself). But there is a growing realisation that trust by proxy is not enough on its own, and that without prejudice to the necessarily secret nature of most of their work, institutional safeguards and direct public engagement are also needed.

The ISC Privacy and Security Report

10.6. Having read the written evidence submitted to the ISC, together with transcripts of the closed oral evidence to it (which was the subject of more penetrating questioning from ISC members than was evident at the televised open hearing at which the three Agency chiefs gave evidence in November 2013) I have no reason to doubt the accuracy of the ISC Privacy and Security Report as a statement of the Agencies' practice and, where applicable, of their views.

10.7. There are a number of respects in which I could have wished for a fuller public statement of the factual position, as it appears that the ISC itself may have done.[3] But I am not generally in a position to publish material which the ISC has recently felt obliged to redact.[4]

10.8. That said, there are respects in which I have now been able to include material that the ISC was not:

(a) Some brief examples of the utility of bulk interception are given at Annex 9 to this Report: the justification to a public audience of such a potentially intrusive power deserves and arguably needs more, but the examples give at least a flavour of the classified instances on which I have been briefed.

---

2 A recent example is the Agencies' procedures for dealing with legally privileged material, disclosed in the Belhadj IPT Case and conceded by the Agencies to be inadequate.

3 The report broke new ground by avowing the use of bulk personal datasets, albeit with little detail (paras 151-163). However no open examples are given of the utility of bulk collection (paras 82-89), of interference with wireless telegraphy (para 173) or of CNE (para 178); and the treatment of what is described as "*another major processing system by which GCHQ may collect communications*" (paras 65-73) is enigmatic. The ISC expressed regret that examples of the effectiveness of bulk interception capabilities could not be published (para 81). It also stated that the Certificate which accompanies the s8(4) warrants should be published (para 101), despite not having been able to do so itself, and that "*all the Agencies' intrusive capabilities*" should be avowed (para 285).

4 Particularly in view of the fact that the Prime Minister is authorised to exclude from this report any matter that appears to him to be "*contrary to the public interest or prejudicial to national security*": DRIPA 2014 s7(7).

(b) I have also been able to summarise, in this Chapter, some submissions that were made to me by individual Agencies about the legal framework in which they operate, and how it might usefully be changed.

The Agencies

10.9. MI5, MI6 and GCHQ are constituted by Acts of Parliament[5] which spell out both their functions and, in conjunction with other relevant statutes,[6] the permitted scope of their activities. Their informative and accessible websites give an idea of their activities, and contain links to the public speeches that are given from time to time by each of their chiefs. In essence, and so far as relevant to this Review:

(a) MI5 finds, investigates and disrupts people who pose threats to the UK, many but not all of whom are in the UK. It seeks the support of the other two Agencies, whose principal focus is abroad.

(b) MI6 collects intelligence and undertakes covert activity globally, mainly using a combination of human and technical sources, in relation to the full range of threats and in support of the UK's foreign, defence and security policies.

(c) GCHQ collects intelligence globally on a large scale about the full range of threats to UK interests, to inform foreign, defence and security policies. It works on the front line of UK intelligence activity and informs work against the threats faced in the UK, which are dealt with by MI5 and the law enforcement agencies.

The Agencies may of course disrupt, deceive or seek to "*turn*" people, and may in some cases be authorised to commit acts (e.g. criminal damage) that would otherwise be unlawful. But they have no police powers (e.g. stop and search, arrest, detention), and are subject in all their activities to the constraints of UK law.

10.10. The Agencies' last financial statement put their combined budget at £2.1 billion.[7] Full-time equivalent staff numbers for the Agencies as a whole were 12,190 in 2013-14, with GCHQ the single biggest employer.

10.11. Secrecy is central to the work of all three Agencies. Whereas law enforcement bodies operate covertly only when they need to – and exude a certain sense of regret that it is ever necessary – the Agencies only exist because of the need to operate in secret. If something can be done openly, the Agencies are not needed to do it.[8] This does not mean that they are ungoverned or unaccountable, nor that the need for their activities to be necessary and proportionate is in any way reduced. It does however

5 SSA 1989 (MI5) and ISA 1994 (MI6 and GCHQ).

6 Notably HRA 1998 and RIPA.

7 *Security and Intelligence Agencies financial statement 2013 to 2014* (June 2014). By way of contrast, the US National Intelligence Program budget for fiscal year 2014 was in excess of $50 billion. The budget of the NSA (which claimed in 2012 to employ more than 30,000 people across the world) is classified, as is that of GCHQ.

8 Of course, the Agencies do some things openly, for example communication security advice at GCHQ and protective security advice at MI5.

create a tension with the legal requirement that the law governing their activities must be accessible and foreseeable. [9]

10.12. But the differences between intelligence and law enforcement should not be over-emphasised. Since 1996, it has been an express function of MI5 to act in support of the activities of police forces and other law enforcement agencies.[10] In the wake of the 2005 London bombings, this was facilitated by the formation of Counter-Terrorism Units across the country where police and MI5 combine their resources in a common cause. Their capacities are to some extent interchangeable, and directed at the same targets. The efficient working together of intelligence and law enforcement is a distinctive feature of the UK security landscape, and one that is noted and envied abroad.

Summary of requirements

10.13. The Agencies saw their main challenge, as the National Security Adviser reported in 2014,[11] to maintain their capabilities in the face of an evolving threat picture and rapid technological change.

10.14. They expressed their priorities to the Review as follows:

Capabilities

(a) To maintain their abilities to access the content of communications, and communications data.

(b) To collect communications in bulk where they cannot refine targeting at the time of collection to individuals' communications; and to use bulk collection where necessary to discover new threats and targets.

(c) To maintain a flexible and agile global reach, commensurate with the Government's foreign, security and defence policies.

(d) To be able to exchange information amongst themselves and maintain their position as part of an international community in the exchange of intelligence.

Legislation and oversight

(e) To be able to operate in secret, subject to Parliamentary and judicial oversight and ministerial control.

(f) To be subject to authorisation arrangements that protect the secrecy of their sources and methods, and which provide timely decision-making.

9 As set out in detail at 5.18-5.24.
10 SSA 1989, s1(4), added by SI 1996/2454.
11 Security and Intelligence Agencies Financial Statement, June 2014.

(g) To be subject to oversight that is sufficiently rigorous to maintain public consent and confidence, without distracting more than is necessary from the performance of their core functions.

(h) Individual agencies also make some specific suggestions in respect of warrantry.

10.15. These priorities are developed in the remainder of this Chapter.

Agency capabilities

10.16. The Agencies depend increasingly on cooperation with each other and with international partners. Against that background:

(a) They seek to acquire communications, by cooperation with service providers or covertly, in order to find information which can lead them to an otherwise unknown or obscured target.

(b) They develop software that enables them to analyse very large amounts of acquired data, to identify linkages and find new targets of intelligence interest ("*target discovery*").

(c) They attempt to overcome encryption and its impact on traditional methods of interception by attacking it with powerful computers, by hacking individuals' electronic devices, by modifying software and by guile, innovation and creativity.

(d) They seek to understand the nature and scale of cyber attack in order to protect Government services online, the UK's Critical National Infrastructure, businesses and individuals.

(e) They seek to operate without being discovered.

(f) They seek to influence their targets' behaviour, by making themselves seem omnipotent or - at other times - weak.

In all this, the Agencies are no different to their counterparts in other democratic countries. But they strive, of course, to be among the best.

Technological change and encryption

10.17. All countries face the same challenges from the development of technology and the communications market, as set out in Chapter 4. The Director of Europol said recently that encryption has become:

> " .. the biggest problem for the police and the security service authorities in dealing with the threats from terrorism … It's changed the very nature of counter-terrorist work from one that has been traditionally reliant on having

good monitoring capability of communications to one that essentially doesn't provide that any more."[12]

10.18. Even the US authorities are unable to access domestically all that they need. The Director of the FBI has referred to this as "*Going Dark*", a challenge which relates not just to the powers available to US intelligence and law enforcement but to how technology is developing, and companies' practices.[13]

10.19. The Agencies forcefully point out that if they cannot maintain their capabilities, threats will go undetected and opportunities to disrupt the ill-intentioned will not be identified. They struggle with the growth of encryption and the diversification of the communications market. It would be wrong to assume that the Agencies have a constant technological edge over their targets, whether through crypto-analytical power, back-door access or partnership with other agencies. Each side has advantages, and neither can be sure of the upper hand: rather, in the words of the Chief of MI6, they are engaged in "*a technology arms race*" in which resourcefulness and creativity are at a premium.[14]

10.20. The Agencies do not look to legislation to give themselves a permanent trump card: neither they nor anyone else has made a case to me for encryption to be placed under effective Government control, as in practice it was before the advent of public key encryption in the 1990s. There has been no attempt to revive the argument that led to the Clipper Chip proposal from the NSA in the 1990s, when public key cryptography first became widely available.[15] But the Agencies do look for cooperation, enforced by law if needed, from companies abroad as well as in the UK, which are able to provide readable interception product.

10.21. The Agencies seek to address impeded access to communications through their own cryptographic work. They will also need to develop new methods of accessing data, for example through increased use of CNE. They therefore want the capabilities and an appropriate legal framework within which this work can be carried out.

Bulk Collection

10.22. The Agencies collect the content and related communications data of external communications in bulk. This has been highly controversial, particularly since the Snowden allegations about GCHQ because it inevitably involves their acquiring material on persons who are not and will never be subjects of interest to them. The argument for this is two-fold.

(a) First, when acquiring intelligence on activities overseas, the Agencies have less ability to identify targets than is the case for security and law enforcement activities in the UK. They argue that they need to collect large quantities of communications in order to find the ones that are of interest. This has

12 "Europol chief warns on computer encryption", BBC website, 29 March 2015.
13 Speech at Brookings Institution, Washington, D.C. 16 October 2014.
14 The Chief's speech to English Heritage, March 2015, MI6 website.
15 See 4.46 above. Under that proposal, a cryptographic key to any device fitted with a Clipper Chip would have been provided in escrow to the US Government, which when duly authorised could have listened to any communication. Whether for technical or political reasons, the idea never took off.

resonance with the argument made by law enforcement in relation to the retention of domestic communications data. The Agencies may begin with a small clue – perhaps a phone number, a suspect location - and from it they can build up the links that will provide the intelligence needed.[16] But they can only do this if they have the communications material available to search for the links.

(b) Secondly, the Agencies' ability to understand what communications bearers will be used by subjects of interest overseas is limited and their ability to access those channels is not guaranteed. Subjects of interest are very likely to use many different means of communications and may change them frequently, some doing so to frustrate their being surveilled. So where a communications channel can be accessed and it is likely to carry communications of interest, the Agencies will make the case to the Foreign Secretary for a warrant to intercept that channel in bulk. This does not however provide the capability to access anything like the totality of internet traffic.

10.23. The Agencies reject the argument that this bulk collection amounts to mass surveillance. This is supported by the findings of the IOCC,[17] the IPT,[18] and most recently the ISC:

> "Our Inquiry has shown that the Agencies do not have the legal authority, the resources, the technical capability, or the desire to intercept every communication of British citizens, or of the Internet as a whole: GCHQ are not reading the emails of everyone in the UK."[19]

10.24. Looking to the future, the Agencies also anticipate that domestic security work will increasingly rely on the use of bulk data, including the examination of communications data within the UK. The spread of encryption and the multiplicity of identities used online by individuals mean that the kind of target search and discovery familiar from overseas operations will be needed in the domestic sphere. They make the point that the internet knows no geographic boundaries and a suspect may be hidden within it as easily in Britain as anywhere else.

10.25. In many respects the use of communications collected in bulk is another aspect to the Agencies' use of other bulk data, which has been openly discussed for the first time in the ISC Privacy and Security Report.[20] Bulk data are available to the Agencies under SSA 1989 and ISA 1994, and exemptions in DPA 1998. As the Chief of MI6 recently put it:

> "Using data appropriately and proportionately offers us a priceless opportunity to be even more deliberate and targeted in what we do, and so to be better at protecting … this country."[21]

16 GCHQ explained this in "How does an analyst catch a terrorist?": 7.5 above.
17 IOCC, *Report for 2013*, 6.5.38.
18 Liberty IPT Case, judgment of 5 December 2014.
19 ISC Privacy and Security Report, Key Findings.
20 ISC Privacy and Security Report, chapter 7.
21 The Chief's speech to English Heritage, March 2015, MI6 website.

Together with other information, bulk data allows a more complete intelligence picture to be drawn. Without it, it may not be possible to discover new threats and follow a lead to a point of closely targeted intervention.

10.26. During my Review, the US National Academies Report on Bulk Collection of Data was published in response to President Obama's request to address whether software could be created to allow the US intelligence community more easily to conduct targeted information acquisition of signals intelligence, rather than bulk collection. The Academies said:

> "No software-based technique can fully replace the bulk collection of signals intelligence, but methods can be developed to more effectively conduct targeted collection and to control the usage of collected data... Automated systems for isolating collected data, restricting queries that can be made against those data, and auditing usage of the data can help to enforce privacy protections and allay some civil liberty concerns…"[22]

GCHQ told me, when drawing this to my attention, that they already practise the additional approaches suggested by the Academies.[23]

Access to communications data

10.27. The Agencies are currently able to obtain communications data, including through their bulk interception powers, and they look forward to the future legal framework maintaining their ability to do so. They face the same problems as law enforcement in obtaining the communications data that they need concerning their targets, particularly from overseas companies but also where data are not currently retained.

10.28. But as the ISC noted (with surprise) in its recent report:

> "the primary value to GCHQ of bulk interception was not in reading the actual content of communications, but in the information associated with those communications".[24]

GCHQ has therefore suggested that there should be a new power to intercept only this information rather than, as at present, all content as well. It points out that such an approach would intrude less into privacy. It also left me in no doubt, however, that the ability to intercept technical elements of communications, such as cookies and web logs (sometimes described as "*content derived metadata*"), which fall outside the definition of communications data in RIPA and so must be treated as content (despite being less sensitive than content as ordinarily understood) was essential to their target discovery work.[25]

22 National Academies Report, *Bulk Collection of Signals Intelligence: technical options*, (January 2015).
23 Letter from Robert Hannigan, 20 January 2015.
24 ISC Privacy and Security Report, para 80.
25 Evidence to the Review, April 2015.

International relationships

10.29. The Agencies point out the importance to British foreign, defence and security policies of their ability to support a very wide range of intelligence requirements. UK intelligence indeed has a remarkable global reach. But to retain this reach, the Agencies argue they must maintain a breadth of capability including advanced technical know-how that enables them to be partners of choice to other intelligence agencies whenever British interests arise. Because those interests change quickly, indeed faster than new intelligence capabilities can be developed, the Agencies must themselves retain a breadth of capability sufficient to react straightaway when demands change. This argument bears particularly on GCHQ, its relationship with the NSA, and its ability to intercept communications globally.

10.30. There is an international trade in intelligence. In the Charles Farr Statement, the Government's argument for intelligence sharing is set out:

> "It is highly unlikely that any government will be able to obtain all the intelligence it needs through its own activities. It is therefore vital for the UK government to be able to obtain intelligence from foreign governments both to improve its understanding of the threats that the UK faces, and to gain the knowledge needed to counter those threats. Indeed, the intelligence that a foreign government shares with the intelligence services (on a strictly confidential basis) represents a significant proportion of the intelligence services' total store of intelligence on serious and organised criminals, terrorists and others who may seek to harm UK national security. The store of intelligence forms a resource for the government in seeking to take preventative action to counter threats, and save lives."

10.31. As discussed at 7.66 above, the strongest partnership is the Five Eyes community involving the UK, USA, Canada, Australia and New Zealand. But there is bilateral sharing with many countries, not all of them in the established communities of the EU or the North Atlantic Treaty Organisation (NATO). Some of these relationships are broadly based where there is an enduring mutual interest. Others come together for a particular purpose such as a joint intervention.

10.32. These international relationships are a vital contributor to their ability to provide the intelligence that the Government seeks. They therefore wish to preserve them within a legal framework that respects the confidentiality other governments require, whilst maintaining domestic confidence in their action. This is another area where the recent report by the ISC has called for future legislation to control the arrangements more explicitly, defining the powers and constraints governing such exchanges.[26]

Techniques and warrants

10.33. MI5 and GCHQ have the leading interest in formulating the needs of the Agencies for investigatory powers affecting communications.

---

[26] ISC Privacy and Security Report, Conclusion TT.

10.34. MI5 described itself as seeking not to expand its territory but to hold its ground:

> "We are certainly not seeking '*sweeping new powers'* or, when taken in the round, an increase in levels of intrusion. But what we do require are powers, approved by Parliament, which allow us to keep pace with the changes in behaviour of our [subjects of interest] and in technology, in order to achieve broadly similar levels of assurance against the national security threat we face."[27]

10.35. MI5 considers that, due to the proliferation of communications platforms and techniques available to those it is investigating, it needs to use a wider range of techniques more frequently to obtain comparable insight. Equipment interference, for example, which may require both a property and an interception warrant, epitomises that need. Access to bulk personal data sets is also becoming more important to its investigative work.

10.36. MI5 has therefore suggested that there would be benefit in enabling the Secretary of State to authorise under a ***single warrant*** all the intrusive techniques she is currently permitted to authorise. Their powers would not extend beyond those which they have currently, and all the interference authorised would need to be justified as necessary and proportionate for the existing purposes. A single warrant would give the Secretary of State and the Commissioners better oversight of the whole of an operation and the intrusion involved, and enable decisions on the proportionality of the interference to be taken in a more informed way. It would also make more efficient use of the Secretary of State's time, and reduce repetition in the number of applications.

10.37. MI5 suggests that the safeguards and handling arrangements for the product of such warranted operations should also be made consistent.

10.38. MI5 has also proposed that its use of ***thematic warrants*** (warrants against clearly defined groupings of individuals who are all carrying out the same activity of concern) be made subject to more explicit safeguards and that current internal policies and safeguards already in place for such thematic warrants be formalised as part of the law or in a Code of Practice. They suggest, furthermore, that their use of bulk personal data sets should be formalised in the same way by introducing more formal published safeguards in addition to the internal processes that already govern them.

10.39. MI5 has concerns that the current provisions for ***schedules to s8(1) warrants*** do not reflect the dynamic nature of internet communications and add to the difficulty of being specific as to which techniques and authorisations might be required. So, for example, it envisages that a warrant might give authority to intercept a named individual's mobile phone communications, but would no longer need to have a schedule which set out the phone number concerned, and would not therefore require modification if the phone number were changed by the targeted individual.

---

27 Evidence to the Review, 17 February 2015.

10.40. GCHQ provided a set of features with supporting justification which it considered essential in future legislation, incorporating:

(a) The continued ability to acquire ***bulk data*** from a variety of sources, including through the use of new techniques, such as CNE, and through the exploitation of commercially available Big Data, to deliver the intelligence requirements of the future. Analysis of bulk data - usually communications data or content-derived metadata (see 10.28 above) - is essential to the discovery of unknown or only very partially understood threats to the UK. As communications technologies evolve, GCHQ's techniques will need to respond and develop accordingly.

(b) The ability to combine such data acquired from a variety of sources and using a variety of techniques into a single intelligence picture. A ***single legislative framework*** covering all of this activity would be preferable to the current mix of arrangements in terms of enabling greater transparency and ensuring consistency, as far as is possible, of authorisation regimes, safeguards and oversight.

(c) The ability to intercept ***communications data and content-derived metadata*** other than as a by-product of content interception. This is not provided for in all circumstances in the current legislation. On average, communications data and content-derived metadata is less intrusive than content, and there are various scenarios and applications - notably but by no means exclusively in the context of GCHQ's cyber defence role - where it is not always necessary to examine content in order to derive intelligence insight. In such circumstances, it would therefore be more proportionate, and clearly preferable, only to acquire the communications data or in some cases the content-derived metadata, and not the whole content.

(d) A ***two-stage authorisation process for bulk data*** (acquisition and access), with the weight of the authorisation burden falling at the point of acquisition, and access to specific data subject to rigorous retrospective review. GCHQ acknowledges the need for, and values, a robust and accountable end-to-end process to govern their exploitation of intelligence material. In the case of bulk untargeted data, they accept that intrusion occurs at two stages: first at the point of acquisition; and then at the point at which material is actually seen or listened to by a human being. The overall framework for authorisation, accountability and oversight must be compatible with an approach to this second stage that achieves target discovery through the agile testing of hypotheses against the full range of available intelligence data, rather than the simple searching for already known target identifiers such as an email address or telephone number. GCHQ argues strongly that this can best be achieved by a rigorous audit process after the event.

(e) An ***explicit basis for sharing data*** with other Agencies and with foreign partners. The ability to share data with both domestic and foreign partners is vital: no single organisation, or state, is able to acquire all the intelligence it

needs to safeguard its national interests. It is important, therefore to ensure that there is a clear and transparent legal basis for such sharing, and the safeguards that apply.

10.41. GCHQ could see benefit in putting serious crime procedures on a par with those for national security, in particular by having warrants last for six months rather than three. It was a point generally made that when warrants last for only three months, it is often necessary to start preparing a renewal application without a full understanding of the impact of the original warrant.

10.42. GCHQ also expressed a clear intention to be more transparent, wherever possible, about its capabilities and operations.

Authorisation

10.43. At present, warrants for ***interception*** are approved by the Secretary of State. Both the Home Secretary and the Foreign Secretary are up-to-date with the requirements placed on the Agencies and the Government's policy and operational needs. They are to a large extent also responsible for them. So there is an easy fit between the Agencies' work and the responsible ministers' portfolios. The Home Secretary bears much the biggest burden among Secretaries of State who approve warrants and she has regarded this as in keeping with her democratic accountability for the actions of the Agencies, a position has been endorsed by the recent report of the ISC.[28]

10.44. The Agencies have made no suggestions to me that the current arrangements for approval by the Secretary of State should be changed. They recognise that there is however pressure to do so from a number of other quarters. Were that to happen, their chief concerns would be to ensure:

(a) the timeliness of a revised approval process; and

(b) arrangements to maintain both security, and sufficient background for the work to be carried out effectively.

Although much of MI5's work may lead to prosecutions in UK courts or to other activity wholly and properly independent of the government, that is not true of most foreign intelligence work. The actions of the Agencies overseas and of the rest of government are properly and intimately connected. The FCO was keen to emphasise that preserving national security, to which purpose most of the Agencies' work is directed, is a function of the executive branch of government, and was concerned that the political and diplomatic context of any action they take should continue to be considered in that context.

10.45. The Agencies are also concerned to maintain their agility, and operational secrecy, in obtaining ***communications data*** from service providers. The recently published Acquisition Code recognises that there may be circumstances where "*ongoing operations or investigations immediately impacting on national security*" mean that

28 ISC Privacy and Security Report, Conclusion GG.

authority to obtain communications data cannot be given independently of the investigation team. Where this is the case, it is to be reported to the IOCC and may be covered in his report.[29] The implication is that these circumstances should be the exception not the rule. The ISC has questioned the validity of any exception for the Agencies. The Agencies recognise the need to address the requirement for independent authority, even though it may require changes to their current working practices.[30]

29 Acquisition Code, 3.13-3.15.
30 ISC Privacy and Security Report, Conclusion HH.

11. SERVICE PROVIDERS

Scope and sources

11.1. This Chapter summarises the submissions made to me by service providers, both domestic and international.

11.2. I received open written submissions from the Internet Services Providers' Association, BT and Vodafone, together with a short joint submission from Facebook, Google, Microsoft, Twitter and Yahoo, each of which I met subsequently (as I did Apple) in London and/or in the US. Confidential submissions were received from BT (again), TalkTalk, EE, Three, Telefonica and Virgin Media. Many CSPs are represented in the Communications Data Strategy Group, two of whose meetings I was invited to attend, and I exchanged views with others at Wilton Park conferences in October and November.[1]

11.3. Service providers do not of course have a single view on the issues with which this Review is concerned. They offer different services in competition with each other and have different business models. Yet there are a number of common strands to their thinking, and on some matters they have made efforts to come to a joint view.

The importance of trust

11.4. All service providers set considerable store by the levels of trust that their customers place in them. For example, the US companies put to me that:

> "… we must earn and maintain user trust, and users expect that their personal communications be treated with the same respect online, as they would be offline."[2]

Vodafone, likewise, told me that "…*the one word we consider to be the bedrock of our business is trust*."[3] Service providers consider that trust is best promoted by protecting their customers' privacy (rather than, for example, going out of their way to assist law enforcement by revealing the details of communications which they have provided).

11.5. However, at 2.28 above, I set out some recent survey figures for user trust, which demonstrate much lower figures than providers want. Indeed, they feel that they have been damaged directly or indirectly by the revelations in the Snowden Documents, and the accompanying perception that they cannot be trusted to protect their customers' data. This, and a wish to make up lost ground, heavily influence their approach to questions of surveillance by governments. The accelerated rate at which some service providers have moved towards services encrypted by default is the clearest example of this over the past two years. Moreover, they are sensitive to the views and criticisms of civil society groups and seek to be better regarded by them in order, at least in part, to help build up levels of customer trust.

---

1 Unattributed quotations in this Chapter are taken from various of these meetings.
2 Joint evidence to the Review from Facebook, Google, Microsoft, Twitter and Yahoo, October 2014.
3 Evidence to the Review, October 2014.

11.6. Of course, and in line with the goal of increasing trust, providers approach the requirements from states for interception and communication data provision with a clear focus on their business needs, which are in turn influenced by current technological and market developments. Vodafone described it succinctly:

> "If our customers begin to believe that their personal communications are no longer private, they will either use our services less or switch to others they believe are more protective of their privacy."[4]

11.7. This approach informs service providers' views on the topic. They stress the importance that they comply (and are seen to comply) not only with national law, but with internationally recognised principles of human rights. As BT explained:

> "We consider that it is appropriate to maintain a regime that permits access to content and communications data, provided that the circumstances are suitably circumscribed, and provided that all necessary checks and balances are in place to ensure the lawful and proportionate operation of that regime, particularly from a human rights perspective."[5]

11.8. However, for service providers operating internationally, complying with the law is a complex demand. They do not see it as their role to resolve the conflicts of jurisdiction that arise when, as is frequent when a law enforcement agency seeks communications data or intercept on a customer, the provider is based in one country, their customer who may or not be under suspicion is another, and the data needed is in a third. But the reality is that providers are at the centre of resolving those conflicts on a daily basis.

11.9. All service providers stress that they are prepared to share data with the authorities in order to save life and prevent crime. But governments in the UK and elsewhere can no longer expect to conduct surveillance of communications on the basis of a cosy, voluntary relationship with a limited number of providers. Service providers are increasingly uncomfortable with voluntary arrangements, and may well show a preference, absent compulsion, to protect customers' privacy rather than cooperate with governments. This gives them a surer base for action. Some service providers will tip off a customer that they are under surveillance unless persuaded not to do so, typically by a court order.[6]

International enforcement

11.10. Before turning to specific views of service providers based in different jurisdictions, it is worth highlighting the most significant issue between service providers on the one hand and the intercepting agencies and users of communications data on the other:

---

4 Evidence to the Review, October 2014.

5 Evidence to the Review, October 2014.

6 For example, Twitter's policy is "*to notify users of requests for their account information … prior to disclosure unless we are prohibited from doing so* ": see Twitter's "Guidelines for Law Enforcement": https://support.twitter.com/articles/41949-guidelines-for-law-enforcement#10.

international enforcement. The issue has its origins in the shift from traditional telephony to internet-based communications.

11.11. A typical-UK based user will have a contract with a company, such as BT, Sky or Vodafone, which provides a telephone line, mobile phone connection or broadband connection. These companies own fixed infrastructure in the UK and may be required (see Chapter 6) to cooperate with the Government in ways that facilitate interception and the provision of communications data. When RIPA became law 15 years ago, these companies still provided the vast majority of UK communications that would be of interest to the security and intelligence agencies or law enforcement.

11.12. That model is changing rapidly and significantly.[7] It can be very difficult to obtain data from service providers, in particular OTT providers which are based overseas and do not store their data in the UK. That is so especially if they are protective of their customers' privacy, or consider themselves inhibited from assisting by their domestic law. The problem has been exacerbated by the common use of strong encryption, which means that the content of communications cannot be read even if the message is intercepted whilst it passes over infrastructure in the UK.

Views of service providers

11.13. It is convenient to look at the views of service providers in two groups: those based overseas and those with UK infrastructure. Although there is overlap in their views, and no complete agreement within the two groupings, they have each reached a broad consensus and discussed it with me collectively.

11.14. A rather specific, yet important, area of complete unanimity worth highlighting was support for the SPoC arrangement (7.39 above), which was said to act both as a "*quality filter*" and as reassurance that there had been "*a lot of checks and balances*". All companies wanted it to be retained and developed. US companies described it to me as "*a model for everyone*" and compared it favourably to the US system, in which they could be contacted by any of "*10,000 FBI agents, who don't necessarily know what they are asking for*".

Overseas service providers

11.15. Shortly after his appointment, Robert Hannigan, who became director of GCHQ in November 2014, wrote publicly about the problem of obtaining interception product and communications data from companies overseas (principally, in practice, the US), and pressed for greater cooperation.[8] Yet the companies for their part regard this as essentially a problem for governments to address. The US companies said to me:

7 See, further, 4.7-4.10 and 4.14-4.16 above.

8 "The web is a terrorist's command-and-control network of choice", the Financial Times website, 3 November 2014.

> *"*Governments should not unilaterally try to compel disclosure of email or other private content across international borders, particularly when that data belongs to citizens of another country*."*[9]

They were united in their opposition to any system in which they could be required to hand even the US Government a key to encrypted material: even if this had been feasible politically it was thought that it would, like the abandoned Clipper Chip proposals which sought maintain access for intercepting agencies in the 1990s, simply encourage new strategies for secure encryption.[10]

11.16. Some foreign companies have made clear their unwillingness to facilitate cooperation with intelligence or law enforcement:

(a) Telegram, which is used by many foreign fighters in Syria, advertises itself heavily as privacy-secure, and promotes "*crypto-contests*" to test the security of its encryption.[11] Its co-founder Pavel Durov, a Russian citizen, is quoted as saying: "*The no. 1 reason for me to support and help launch Telegram was to build a means of communication that can't be accessed by the Russian security agencies*."[12]

(b) Apple has put its encryption beyond its own reach. It says of its messaging service: "*Apple has no way to decrypt iMessage and FaceTime data when it's in transit between devices. So unlike other companies' messaging services, Apple doesn't scan your communications, and we wouldn't be able to comply with a wiretap order even if we wanted to*."[13]

Others, while understanding the importance of national security, feel discomfort about bilateral negotiations with the UK Government because they are sensitive, post-Snowden, to allegations that they are voluntary participants in privacy intrusion. As one company put it to me: "*We can't get into conversations that leave our customers on the outside ...our priority is our brand, not UK intelligence*".

11.17. The Government has asserted the extraterritorial effect of UK law, and made it explicit in DRIPA 2014. In theory, therefore, the Government could seek to compel cooperation by overseas service providers in the same way as it compels companies based in the UK, although this has not yet been tested in a UK or foreign court. In a narrow sense, this might be said to meet the desire of the US companies for legal clarity. But overseas service providers are generally unhappy with the assertion of extraterritoriality in DRIPA 2014, which they did not necessarily accept (despite the view of the UK Government) to have been implicit in the previous law and had not encountered in the laws of other countries. While legal compulsion was in principle preferable to voluntary compliance, it was thought that the unilateral assertion of extra-territorial effect would be met by blocking statutes, was not "*scalable to a global*

9 Joint comments from Facebook, Google, Microsoft, Twitter and Yahoo, October 2014.
10 See 4.45 above.
11 See https://telegram.org.
12 "Why telegram has become the hottest messaging app in the world, The Verge website, 25 February 2014.
13 See the privacy section on Apple's website: https://www.apple.com/uk/privacy/privacy-built-in/. Its comments do not however apply to encrypted data on the iCloud.

approach" and was viewed as "*a disturbing precedent*" for other, more authoritarian countries.

11.18. In practice, engagement with overseas companies has to date been entirely on a voluntary basis, although it is necessary for the UK agencies to acquire the appropriate legal instrument, an interception warrant or communications data authorisation or notice, before they seek the cooperation. The degree of cooperation diminished generally post-Snowden and varies between companies and between data types. Thus:

(a) Where interception is concerned, many US companies consider themselves to be constrained by federal law limiting voluntary disclosure to cases in which a provider reasonably believes that immediate disclosure is required by an emergency involving "*imminent danger of death or serious physical injury*".[14] While this might allow service providers to assist e.g. in cases of kidnap or bomb threat, many serious investigations (including terrorist investigations) do not satisfy these criteria.

(b) The sharing of communications data is less legally constrained, with the result that service providers can accede to simple requests to verify subscriber identity, though this is not universal.

(c) There are also issues at the margins where companies can make their own interpretation of the dividing line between content and non-content.

There have been recent and limited signs of improving cooperation, driven in part by the spread of ISIL and its dependence on social media. But it is also relevant to note that many OTT providers in Silicon Valley and elsewhere are small and relatively new companies, often with a strong libertarian ethos and without the legal or regulatory expertise to deal on an informed basis with requests from foreign governments.

11.19. A number of major US companies, accustomed to the FISC procedure in the US, disliked the notion of authorisation by the Secretary of State and indicated to me that they would be more comfortable about complying with a warrant if it were judicially authorised, providing "*another pair of eyes that is separate from the investigative apparatus*". While it was appreciated that other sorts of independence could be built into the system, "*the UK is in a minority with political authorisation, and perceptions do matter*". It was also felt that "*improving RIPA*" in this way would "*set a good guide for other jurisdictions*". One major company went so far as to suggest that if the UK introduced judicial authorisation, more cooperation would be forthcoming, though I was not left with the impression that this was a universal view.

11.20. The overseas service providers with whom I discussed the matter apply their own judgement to a request put to them from the UK before they comply with it. Some companies have published transparency reports, which show their assessment of how many requests from the British authorities they have met.[15] The figures for rejection of

[14] 18 US Code §2702.

[15] E.g. Google, http://www.google.com/transparencyreport/; Yahoo, https://transparency.yahoo.com; Twitter: https://transparency.twitter.com.

British requests are difficult to interpret. Some may be rejected because the data does not exist, though the UK authorities will also suppress demand where they feel that it will not be met. Companies will reject requests which they feel are illegal in their host jurisdiction, or which they believe it would be unethical to meet, for example where the interests of a third country might be adversely impacted. I was shown evidence from a British agency that at one point in 2014 about 75% of the desired intelligence coverage for a particular operation could not be obtained from service providers.

11.21. In their discussions with me, the US companies advocated the adoption of the Reform Government Surveillance Principles,[16] which they have been creating as part of the Global Network Initiative, a multi-stakeholder group of companies, civil society organisations investors and academics *"working to protect and advance freedom of expression and privacy in the information communications and technology sector*".[17]

11.22. The companies argue that the challenges articulated by the British government are global problems and require a global solution. The Reform Government Surveillance Principles are not directed specifically at the UK. Nevertheless aspects of current British law and practice (most obviously, bulk collection) would not meet the principles.

11.23. The US companies emphasised to me that the UK is influential and should lead internationally in this sphere. But its influence should be exerted at the inter-governmental level, not by unilateral acts such as the assertion of extraterritorial effect or requiring the local storage of data (data localisation), which would carry security risks, impose huge costs in terms of compliance, network architecture and engineering and render the internet slower and less efficient.

11.24. The jurisdictional position is indeed complicated. Although many of the companies concerned point to inhibitions in US law, which prevent automatic cooperation with British government requests, some keep data relevant to UK customers in third countries: for example Yahoo and Microsoft do so in Ireland. The companies point out the pressure that they are under to ensure that their operations are human rights-compliant, for example through the United Nations Human Rights Council's adoption, with UK and US support, of the Ruggie principles.[18] They expressed concerns that unqualified cooperation with the British government would lead to expectations of similar cooperation with authoritarian governments, which would not be in their customers', their own corporate or democratic governments' interests.

11.25. Improvements to the MLAT process to obtain intercept and communications data are strongly advocated by the US companies, who would prefer to see the problem resolved by negotiations between governments: "*We are under no illusions that it is perfect*. *But it would be premature to rule it out as part of the solution.*" They claimed

---

16 These can be found at https://www.reformgovernmentsurveillance.com/, and cover (1) limiting governments' authority to collect users' information (including a statement that governments "*should not undertake bulk collection of internet communications*"); (2) oversight and accountability; (3) transparency about government demands; (4) respecting the free flow of information (e.g. by not requiring infrastructure to be located locally); and (5) avoiding conflicts among governments (e.g. by MLAT processes).

17 Global Network Initiative submission.

18 See the UN Office of the High Commissioner, "Guiding Principles on Business and Human Rights", 2011, HR/PUB/11/04.

to look favourably on requests for data preservation, so as to ensure that at the conclusion of the MLAT process the data would still be there.

11.26. But there is little dispute that the MLAT route is currently ineffective. Principally this is because it is too slow to meet the needs of an investigation, particularly in relation to a dynamic conspiracy. For example a request to the United States might typically take nine months to produce what is sought. The MLAT route also does not address intelligence needs. Progress has however been made in discussions with the Irish government in the context of the EU protocols for legal assistance to enable speedy turnaround of warranted interception requests in serious crime cases. There are also plans to introduce electronic document exchange with the United States, which will remove some of the delays inherent in relying on the transfer of hard copies.

11.27. To address this problem of overseas enforcement, at the same time as my Review was established, the government appointed Sir Nigel Sheinwald to be the Prime Minister's special envoy on law-enforcement and intelligence data sharing. Sir Nigel's overarching objective, through discussions with governments, other key international partners and service providers, was to improve access to and sharing of law enforcement and intelligence data in different jurisdictions. Sir Nigel was seeking to identify ways to take forward the British government's relationship with telecommunications companies and explore how new formal arrangements could improve data access and sharing in both the short and longer term.[19] I have been kept informed of his progress.

11.28. A number of options are under consideration which might improve the level of cooperation between US-based companies and the British Government. Some depend on the US Government interceding with US companies on behalf of the British Government. These will require the appropriate political will in Washington as well as the British Government to respond to concerns. There is no immediate solution in sight.

UK service providers

11.29. Most of the areas of concern expressed by NGOs, discussed further in Chapter 12, found some echo in the views on future arrangements volunteered by UK companies.

---

[19] Specifically, Sir Nigel Sheinwald's task, as set out in a Cabinet Office Press Release, 19 September 2014, was to:

- identify ways to take forward the British Government's relationships with the telecommunications companies and ensure that the British Government's work in this area is coherent with its broader relationships with the telecommunications companies, and vice versa;
- explore how new formal US/UK arrangements could improve data access for the UK agencies;
- work with the US government and telecommunications companies on a range of options for strengthening arrangements and ensuring reliable access, e.g. through MLAT systems, other legal or political frameworks or remedies, better arrangements for direct requests from the UK agencies to the companies which hold the data, or other means;
- consider wider international arrangements in this area; and
- ensure that any new arrangements observe the requirement that data are requested and provided only where necessary and proportionate for the purposes of national security and the prevention or detection of serious crime.

Some of these are also mirrored in the Reform Government Surveillance Principles. In particular, some service providers emphasised the need for:

(a) judicial oversight of interception;

(b) greater controls on bulk collection;

(c) further controls on the intrusive aspects of communications data access such as location tracking;

(d) increased transparency (particularly from the government);

(e) strengthened accountability; and

(f) government to take the lead on resolving jurisdictional conflicts.

11.30. UK companies were nevertheless generally sceptical of the prospects of a new single international regime, as advocated in the Reform Government Surveillance Principles, and would be concerned if it increased compliance costs or other reforms had an impact on their competitive position.

11.31. Whilst there was no unanimity on desirable changes in oversight and approval practice, there was an expectation that change would be required to satisfy increasing demands for privacy.

11.32. The UK companies were generally united on a number of other points, which I discuss below.

(a) The current arrangements for cost recovery by companies undertaking interception or providing data were widely applauded and, whilst there was some wish for them to be improved from the companies' perspective, their existence was seen as a strength of the UK arrangements that should be preserved.

(b) The cost recovery arrangements do not however entirely offset a widespread concern by UK-based companies that investigatory powers arrangements could adversely impact on their competitiveness. I was told that government surveillance requirements do have a significant technical impact. Companies were concerned to preserve what they would regard as a level playing field in the market: in other words, that the burden of complying with investigators' needs should not fall disproportionately on UK-based providers, or certain UK-based providers. This was one of the major concerns with the 2012 Communications Data Bill. I was repeatedly told that it was not the job of UK companies to resolve the challenge of encryption of communications carried on their infrastructure, even if they could. They were therefore generally opposed to having to store third-party data in their systems, in the way that had been proposed in the 2012 Bill. The thrust of their concerns was that the Government should by whatever means press the OTT providers to play their full part in meeting the surveillance requirement.

(c) Companies were all concerned about the implications of being compelled to cooperate in interception and data matters. Although they would welcome an avenue to seek clarity, particularly about the meaning of the law and general requirements placed on them, they did not wish to have a discretion to question the merits of a particular interception or data request. It was for Government to ensure that a request was lawful, necessary and proportionate, such that they could then comply with it without fear of redress unless they themselves made an error.

11.33. All thought the Government-industry relationship needed improvement. Some companies were nevertheless suspicious that competitors enjoyed privileged relationships with Government, though no company felt that it had one.

11.34. In this respect, whilst the existing mechanisms of the Government-industry relationship, such as the Communications Data Strategy Group, were welcome, they did not extend to matters of interception.[20] There was an appetite for more strategic discussion with industry at an earlier stage. The perceived inadequate consultation over the 2012 Bill still rankled,[21] as did the handling of DRIPA 2014. There remained concerns that the technical features of the 2012 proposals, the request filter and DPI, were not likely to be effective, though this may be an example of inadequate engagement rather than a fully informed disagreement on technology. They noted that the sunset clause in DRIPA 2014 s8(3) will operate from the end of 2016, and that consultation with them thus needs to begin quickly.

11.35. There was further concern that the law was complex, that it had not kept up with technological and market change, and that it was dispersed over different statutes. Some concerns were highly technical, such as the impact of the definition of interception in relation to requests to remove offensive material or apply virus protection tools. In part the response to these difficulties was a desire to have a route to clarify the law, perhaps through easier access to the courts. But there was an appetite to see the law made clearer and consolidated, for example as between the scope of RIPA and TA 1984. In addition, they felt that data retention and data protection rules could find themselves in conflict.

11.36. UK companies generally thought the distinction between communications data and content was still valid, but needed development. Web logs, cloud services and social media were particularly difficult areas to reconcile with the current definitions. Companies felt that some communications data was highly intrusive and this was not fully recognised by current legislation. There was no longer any simple physical separation of internal and external communications.

11.37. Companies had a number of tactical suggestions as to how interception and data arrangements could be improved within the current legal framework, and believed that greater cooperation would engender ideas for more effective use of available powers and capabilities and enable future challenges better to be anticipated and dealt with.

---

20 Although new arrangements are to be introduced from May 2015, see 7.74.

21 That perception was shared by the JCDCDB, which was critical of the lack of consultation: JCDCDB Report, chapter 4.

11.38. A number of specific suggestions emerged from the special meeting of the Communications Data Steering Group, where the companies and law enforcement and worked together. These were:

(a) Data that does not originate or terminate on the CSPs' network should be considered "*third party data*", not for the CSP to store and disclose.

(b) Consideration should be given to limiting disclosure of retained communications data in civil cases where that goes beyond the purposes for which the data had been retained.

(c) Legislation should require continued consultation between law enforcement and CSPs, so as to ensure that law enforcement can obtain the necessary information by the most effective means, without dictating the precise methods to be used by CSPs to produce it.

(d) Communications data should be redefined to include user data on the one hand and use data on the other, to create a simple and transparent division between the person who is accessing the internet or making a communication and the usage data which is inherently more private and would detail and individuals' activities.

(e) Content should be defined, so as to ensure there is no ambiguity over their obligations to produce material, particularly when stored in the cloud.

12. CIVIL SOCIETY

Sources and scope

12.1. In the course of this Review, I met and received submissions from NGOs, academics, campaigning organisations, activists, trade bodies and others, in the UK and also in the US (listed at Annex 3 and Annex 4 to this Report and referred to for convenience as civil society) who shared with me their views regarding the investigatory powers regime. In a good many cases, those submissions were the start of a dialogue which I have found illuminating.

12.2. Space does not permit a comprehensive account of those submissions, some of which are extremely valuable surveys in their own right. This Chapter aims only to summarise the criticisms, and associated proposals, that were made by civil society to the Review. The reader who wishes to know more is encouraged to read the original submissions, which are published (with the authors' consent) on my website.

12.3. An important (though perhaps obvious) point to make at the outset is that these submissions are not necessarily representative of the views of the public as a whole. Most of those who have been moved to write are well-informed. Many of them have a passionate belief in the importance of privacy, or of limiting the actions of the state. Some are frankly suspicious of the motivations of the agencies and police, and believe that the exercise of intrusive powers, particularly in the absence of suspicion, is liable to do more harm than good. But not everybody shares those views, as demonstrated by the surveys cited at 2.25-2.35 above. Some will always argue for security to be prioritised over privacy; and a great number (including some who could claim to be well-informed) are not particularly struck by imbalance or injustice in the current arrangements.[1] Those positions are only lightly represented in the submissions I have received from civil society.

12.4. A wise legislator will proceed however on the basis that the legal framework governing investigatory powers must be sufficiently robust to satisfy not only those who are easily satisfied, but also those who are suspicious of government or who feel deeply any intrusions into their privacy.[2] In that context, the views expressed below are of particular interest and relevance.

Transparency

12.5. At a general level, concerns with the RIPA regime are far from new. However, they have taken on a new and renewed intensity following the leaks in the Snowden Documents. The allegations in those papers took many by surprise, as have subsequent disclosures by the Government regarding the extent of the investigatory powers used by public authorities. A number of submissions made the point that the alleged conduct should have been clear on the face of the law, or should have been highlighted by the various oversight regimes set up under RIPA and related

1 That is also, generally speaking, the position of those who are appointed to regulate the exercise of investigatory powers and who, because of their privileged access to secrets, are best equipped to understand how they are used: IOCCO, the ISC and the IPT.

2 That is so, particularly, given the international dimension: see 1.9 above.

investigatory powers legislation. The fact that significant public information is only available due to these leaks, of which a significant majority remain NCND, is seen as unsatisfactory.

12.6. This reflects a fundamental imbalance. Those involved in investigatory powers have (naturally) far more information regarding the use of those powers than those in civil society. Yet, as explained by Dr. Paul Bernal: "*[i]t is not enough for the authorities just to say 'trust us': the public needs to know that they can trust the authorities"*. For many, that trust has eroded, and greater transparency is needed to get it back. Indeed, following the judgment of 6 February 2015 in the Liberty IPT case, which held that the failure to make certain procedures public rendered the data-sharing regime unlawful, many saw the need to make more information available to the public. This need for further transparency is a fundamental concern of many of those with whom I discussed these issues.[3]

12.7. The transparency of laws and the public trust in them is not helped (it was suggested) by the "*rushing*" of statutes such as DRIPA 2014 through Parliament, or by piecemeal additions and amendments to those laws, including most recently CTSA 2015. This restricts proper and detailed scrutiny of the measures proposed.

The need for clear legal powers

12.8. It has become increasingly apparent during the course of this Review that a range of techniques and methods is utilised (in particular by the security and intelligence agencies). Some of these intrusive practices do not find clear and explicit basis in legislation, other than general powers in SSA 1989 and ISA 1994. They include:

(a) the use of CNE, only recently acknowledged by the Government through the publication of the Draft Equipment Interference Code;

(b) the suggestion in the Snowden Documents that the security and intelligence agencies are seeking to break encryption standards;

(c) the use, such as there is, of OSINT; and

(d) the use, such as there is, of other surveillance instruments available to the public, such as IMSI catchers.

12.9. A number of those with whom I met, particularly those with a detailed knowledge of the technology involved, expressed serious concern regarding the fact that such powers were apparently used but were not clearly articulated on the face of the legislation.[4] In their view, the use of techniques and methods without, at the least, published guidance, still less explicit Parliamentary approval or public awareness and support, was not only a large issue for society, but ran contrary to the rule of law (and

[3] Access' submission to the Review contains detailed consideration of the issue. However, Robin Simcox's submission urges recognition of the importance of secrecy in the face of national security threats.

[4] Privacy International explained in some detail its concerns in this regard.

possibly the requirements of Article 8).[5] Moreover, the lack of clear statutory authority for such powers insulates them from public-facing oversight.

12.10. These issues arise in particularly acute form in relation to bulk collection, for which the power is (in the views of many) far from apparent on the face of RIPA. Though bulk collection, it is claimed, dwarfs the regimes for targeted interception and acquisition of communications data, its use was largely unknown until recent revelations. This lack of clarity engages questions of whether or not such collection is "*in accordance with the law*": the IPT held that it is (in the Liberty IPT Case, judgment of 5 December 2014). Along with the claimants in *Big Brother Watch and others v UK*,[6] the claimants in the Liberty ECtHR Application have raised the point before the ECtHR.

12.11. In the light of this, I spoke to many activists who emphasised that if broad powers such as bulk collection are to be authorised (a question which is considered below), these must be set out in legislation after proper and public debate. As stated by Liberty, while it is not expected that all the detail of investigatory methods will be published, "*a clear understanding of the absolute limits of what is permitted by legislation is essential when the exercise of powers will be done largely in secret*". Thus many suggestions have urged the publication of further guidance, worked-through practical examples, or legal advice interpreting the law or authorising the powers involved. This, it is suggested, is likely to engender greater trust in the actions of the authorities, which would be operating on powers explicitly set out in legislation and whose actions could thereby be reviewed.

The need for evidence

12.12. Linked to this issue is a central concern of many civil society groups: that they have minimal, if any, evidence of the need for (rather than desirability of) the powers exercised by public authorities. They are of the view that, following the approach of the ECtHR set out in Chapter 5 above, interferences with rights may not be justified unless a justification is provided for that surveillance which is proportionate to the intrusion involved. Moreover, it is important democratically to have public understanding of the need for surveillance, as highlighted by DEMOS. Rights Watch (UK) made the point that "*[t]his is particularly important among communities who are considered suspect due to the involvement of some of their members with terrorist activity*".

12.13. Many challenge the premise of the need for further powers, or even all existing powers. In particular, they note that:

5 In relation to CNE, the legality of the use of these powers is currently under challenge in the PI IPT Case.
6 Application no. 58170/13.

(a) Detailed review mechanisms in the United States have concluded that US programmes were "*not essential to preventing attacks*"[7] or had "*no discernible impact"*.[8]

(b) This is said to be particularly acute in relation to data retention, on which in Access' words, US authorities have "*dithered"*, and without which law enforcement still seems to operate e.g. in Germany.

(c) The key issue for authorities should not be gaining more information, but rather ensuring that information which the authorities do possess is put to good use (an area which could arguably be improved).[9]

12.14. In the absence of adequate justification, it is said that people are being asked to put their faith in a system which they are told is necessary, but with no concrete examples of why that is the case. Examples are demanded, which should demonstrate that the methods successfully employed would not have been successful under a different and less intrusive regime.

Tools for understanding

12.15. Related to this issue is the need for transparency in the operation of the system. Particular concerns in relation to this include the following:

(a) Reporting mechanisms (including Commissioners, the ISC and indeed this Review) must first place their reports before the Prime Minister, who can redact certain sensitive information.

(b) RIPA s19 provides for an offence of unauthorised disclosure of the existence and contents of warrants for interception, which restricts notification in individual cases and hampers the provision of statistics.

(c) The provisions for notification in the Acquisition Code at 8.3 are too restrictive, requiring "*wilful or reckless failure"* simply to inform a party of the "*existence of the Tribunal and its role"*.[10]

(d) Statistics are insufficient and incomparable between bodies, leading to an incomplete and distorted picture. [11]

(e) NCND restricts the information available to the public.

12.16. A number of submissions sought to deal with these points, and I was urged to address each of them. In particular, in relation to statistics, the need for mandatory and clearly regulated publication of statistics by each public authority on the use of such powers, particularly as regards interception and access to data, was highlighted.[12] While the

7 The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, (December 2013), p 104.
8 New America Foundation, *Do NSA's bulk surveillance programs stop terrorists?* (January 2014).
9 See the submissions of Big Brother Watch and Liberty.
10 A point highlighted by IOCCO in its submission to the Review.
11 Again, a matter which IOCCO also raised as a concern in its submission.
12 See for example the submission by the Global Network Initiative.

increased provision of transparency reports by service providers was noted, further submissions highlighted the need for a more permissive regime to allow service providers to report,[13] or the need for regulated standards for and increased mandatory reporting. As well as such mandatory provision, increased detail in the statistics released was also urged,[14] particularly in relation to:

(a) increased reporting of and detail as to the purpose for which data is requested (for both interception and communications data), set out in clear and specific categories;[15]

(b) the specific use to which data is put;

(c) the amount of data collected pursuant to each warrant or authorisation as well as the number of individuals affected;

(d) greater depth as to what kind of person is targeted and why; and

(e) information on rejections of applications.

12.17. More broadly, many are of the view that the public authorities could make significantly more information available regarding the way that they operate.[16] While some argued for a detailed unclassified description of the scale and scope of activities undertaken, others sought more specific information, including sample selectors, target acquisition rules, exemplary warrants, procedures for data minimisation and the length of time for which data is stored. Alternatively, security and intelligence agencies could publish concrete policies or at least summarise the legal advice or assumptions on which they are operating. This would allow review and, if necessary, challenge of the legality of the system.

12.18. Finally, some of the submissions highlighted the need for mechanisms to allow more individuals to gain sufficient information to be able to challenge actions undertaken against them. This includes notification of those wrongly targeted by surveillance,[17] as it was noted that in a number of jurisdictions such a duty exists and operates successfully,[18] as well as the lifting on the ban on the use of intercept material at trial. Again it was urged that this would create greater opportunity for further scrutiny of any wrongful acts.

---

13 As set out in the submissions from Access, Peter Gill and the Global Network Initiative.

14 By, in particular, Big Brother Watch.

15 Steps have already been made by IOCCO in this regard, which published statistics for communications data in the *IOCC Report* (April 2014), and both communications data and intercepted material in 2014 in the *IOCC Report*, (March 2015). This represents an improvement, although the statistics are limited: for interception in particular the statistics were at a high level of generality (it was indicated that 31% of warrants related to national security, 68% to serious crime, and 1% to a combination).

16 See for example the submissions of the Global Network Initiative and DEMOS.

17 As urged by, for example, Human Rights Watch, the Global Network Initiative and Liberty.

18 According to the submission I received from the Bingham Centre for the Rule of Law, this includes Belgium, Bulgaria, Canada, Germany, Ireland, the Netherlands, New Zealand, Sweden and the United States. However, I note that in the Report of Ben Emmerson QC, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397, it is noted that "*very few States*" have provisions for such ex post notification, at para 50.

Coherence and clarity

12.19. Investigatory powers and practices often involve secret, or covert, actions. The importance of coherence and clarity, a desirable feature in any area of the law, is heightened in this context.

12.20. Unfortunately, however, RIPA itself is complex, fragmented and opaque. It is extraordinarily difficult both to understand and to apply. To summarise the concerns in this regard:

(a) As set out in Liberty's submission, "*a striking feature of RIPA is that it treats the various forms of surveillance in a patchy and inconsistent manner"*.[19]

(b) Many of the concepts are outdated, including in particular the apparent distinctions between external and other communications, and content and communications data.

(c) The terminology lacks clarity, in that:

- Important concepts such as "*content*" are not defined.
- Further terms, such as for example "*communications"* and "*subscriber data"* now appear anachronistic and counter-intuitive.

(d) Rules in the legislation and accompanying Codes of Practice are insufficiently detailed.

Single and simple framework

12.21. RIPA itself contains inconsistencies which have been pointed out to me:

(a) Surveillance with a similar purpose but with slightly different methodologies may fall under different regimes, such as for example;

- a conversation recorded by a hidden microphone in a person's home, a hidden microphone in a person's phone itself, and intercept of the conversation;[20] and
- putting a "*tail*" on someone and determining the movements of a person and with whom they have met via the use of geo-location data.[21]

(b) Different safeguards and authorising mechanisms apply to each, leading to possibly counterintuitive results. It was pointed out by those acting for a number of women who had relationships with undercover police officers that the intrusion in their daily lives only had (at the time) to be authorised by a middle-

19 The differences and complications inherent in the scheme as a whole are considered in detail in JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age,* (October 2011).

20 Authorised, respectively, under RIPA Part II, either the Police Act 1997 Part III or ISA 1994 s5, or RIPA Part I Chapter 1.

21 Authorised, respectively, under RIPA Part I Chapter 2 and RIPA Part II.

ranking officer, whereas to listen in to one phone call would have required a warrant from the Secretary of State.[22]

(c) Moreover, there is overlap between different regimes, undermining the safeguards attaching to some. For example, internal communications are intercepted under s8(4) warrants, as are significant volumes of communications data (discussed in more detail in Chapter 6 above).

12.22. The proliferation of other statutes providing for investigatory powers magnifies these concerns. In particular:

(a) How and when other regimes should trump the regime set out in RIPA or vice versa is far from clear. As the scrutiny applied under different regimes may be of differing levels, this raises concerns that a regime with lesser scrutiny may be chosen to perform the same (or a very similar) function.

(b) The extent of the array of different powers is unknown and often ungoverned by supervisory mechanisms.

(c) For many of these statutory powers, minimal safeguards appear on the face of the legislation (e.g. TA s94).

(d) The extent of the intrusion does not match up to the degree of scrutiny applied to the decision. It is argued that similar protection should be given under RIPA to that given to the search of a house, as the nature and extent of the information involved is similar.

(e) As pointed out in the submission I received from Roke Manor Research Ltd, varying capabilities and investigatory techniques are beginning to converge with the advent of technology.

12.23. In light of the above, there was overwhelming support in the submissions I received from civil society for simplifying the statutory framework. The Bingham Centre for the Rule of Law, which in its submission deals extensively with this point, urges:

> "A single, comprehensive statutory framework should govern the use of intrusive surveillance powers by public bodies. In particular, no public body should have the power to access communications data save by way of this framework".

For many, this view extends to all surveillance powers, including those currently set out in or covered by in the Police Act 1997, ISA 1994, SSA 1989, and the different intrusive techniques in RIPA Part II. While conceptions of how such a scheme would operate vary, some have suggested a scheme analogous to that of PACE: a broad statutory framework containing the key elements of what is considered lawful, under which detailed Codes of Practice, more easily updated, can be set out.[23] Professor Peter Sommer in his submission focused on the intrusion that each power would cause, suggesting that the greater the intrusion the greater the scrutiny and

22 See 8.18-8.19 above.
23 As explained in detail by Professor Peter Sommer.

safeguards would need to be applied. Other suggestions for codifying surveillance according to simple distinctions focused on the type of surveillance, such as separate regimes for covert and overt surveillance, or for directed and intrusive powers. However, most focused upon the need for an overarching and simple regime at least in relation to interception and acquisition of communications data, which forms the focus of the remainder of this section.

Remove outdated concepts

12.24. When RIPA was designed, the internet was a rapidly growing and increasingly important means of communication. However, it has been consistently highlighted to me that RIPA has been overtaken by developments in technology, such that in the view of many it is no longer fit for purpose. In particular, the volume and quality of information contained in and in relation to communications has increased exponentially. The distinctions laid out in the regime are increasingly defunct, particularly in light of powerful tools for composite analysis. Unsurprisingly, therefore, many in civil society advocate their removal.

12.25. The first key distinction which many have suggested removing is that between internal and external communications, which is discussed in Chapter 6. While the precise interactions of the different subsections of s8 is opaque, s8(4) warrants (which I term "*bulk"* warrants in Chapter 6), can only be granted for the interception of "*external communications*", defined in s20 as a communication "*sent or received outside the British Islands"*, and accompanying conduct necessary to undertake to seek such interception, under s5(6). This is a very wide power, by comparison to the power to intercept the communications of a single person or connected to a single premises (which I term "*targeted"* warrants in Chapter 6). Many or most of the submissions received referred to those two powers as the power to issue "*internal"* and "*external*" warrants. In practice, as set out in Chapter 6, s8(1) warrants may target both internal and external communications and s8(4) warrants frequently intercept internal communications (though they may not target them). The distinction between the two categories of warrant is said to be either pointless or misleading, for the following key reasons:

(a) As a starting point, what is classified as an "*external communication"* is unclear, as set out in detail in the submission of Graham Smith. Many are of the view that the definition put forward by the Home Office in the Charles Farr Statement is inconsistent and overbroad.[24]

(b) The distinction is outdated in the context of internet communications that are routed (and intercepted) globally.

(c) It is particularly irrelevant in a situation when it is impossible, in practice, to intercept external communications without intercepting internal ones as well (RIPA ss8(5)(b) and 5(6)(a)). Many of the submissions felt that s16 did not do enough to maintain that distinction.

[24] See for example the submissions of Big Brother Watch and the All Party Parliamentary Group on Drones.

(d) It is arbitrary, since it is often impossible to tell at the moment of interception whether a communication is "*external*" or not.

(e) Some are further concerned that the distinction is discriminatory (both in relation to those abroad and to minority groups *within* the UK).[25]

(f) The operation of s16 is far from clear. There is concern from some that the protection it offers may be more apparent than real; as it appears to provide for considerable searching and examination of data on those within the UK, as long as the selection is not on the basis of a factor referable to an individual known to be in the UK.

12.26. Thus, many of the submissions I received were of the view that the distinction should be abolished. In particular, it was said that this would: i) prevent any discrimination or unnecessary difference in treatment based on nationality or geography; ii) remove the arbitrariness and illogicality of the distinction in a world of globally routed communications; and iii) clarify what exactly is undertaken pursuant to different warrants. In answer to the point that some distinction based on either citizenship or geography appears ubiquitous in surveillance regimes globally, actors suggest that this should not stop the UK becoming a leader in this field by expunging the distinction. At the very least, most would urge a publicly developed and technologically sound distinction.

12.27. Many submissions also highlighted the need to expunge the distinction between the content of communications and communications data, a distinction which is said to be artificial.[26] That distinction was premised on an assumption that content is more personal, more valuable, and more private than communications data. But that is now challenged:[27]

(a) The volume of communications data has increased exponentially, and there are increasingly sophisticated means of data analysis which can provide significant information through combining and matching data.

(b) This is matched by the increased utility, richness and inherent privacy of information contained in communications data. As explained by Open Rights Group, there is a qualitative difference in the type of communications data that is available now to that which was available 15 years ago.

(c) It may also be the case that in the context of internet communications the distinction is less clear in terms of determining what is content and what is communications data.[28]

---

25 A concern highlighted by Rights Watch (UK) and the Equality and Human Rights Commission.

26 As set out, for example, in submissions by the Guardian Media Group, the Equality and Human Rights Commission and Liberty.

27 This view is one gaining in prominence: in the recent SURVEILLE Report, it was noted that "*the distinction between "content data" and metadata …is rapidly fading away in modern network environment"* , p. 4.

28 As raised by, amongst others, IOCCO.

12.28. Many submissions were of the view that this distinction should be abolished. At the very least, even if there is some relevance to such a distinction, the justification for two entirely separate regimes is not apparent. As with the internal/external distinction, the commonality of such a distinction in other regimes was not seen as a reason to preserve it in the face of illogicality.

Simplify and define important concepts

12.29. There are a number of elements of the regime which many regard as opaque, and which could be clarified, defined and explained. These include, e.g.:

(a) the extent to which s16 permits the selection of and access to internal communications, which currently is far from clear, and some argue in essence provides a "*third type of warrant*";[29]

(b) what is an "*external"* communication;

(c) what is included within "*content"*;

(d) the factors to be considered in determining whether interception is "*necessary and proportionate"*;

(e) the system to be put in place where the requisite Secretary of State is not available to sign a warrant for interception;

(f) the operation and scope of the newly avowed "*thematic warrants"*;

(g) the different categories of communications data, including perhaps a specific definition of geo-location data;[30] and

(h) the operation and extent of the extra-territoriality provisions introduced by DRIPA 2014.

12.30. These clarifications must be, it is argued, sufficiently detailed to allow civil society and others to see on the face of the statute, Code of Practice or published guidance what is permissible and what is not. Submissions pointed to the use of RIPA to gather the communications data of the Tom Newton Dunn, the political editor of the Sun newspaper, as an example of insufficient detail leading to practices which do not have broad support and which were not generally understood to be within the scope of the legislation.[31] This is a matter which is to be considered by the IPT.[32]

12.31. Moreover, if investigatory powers remain authorised by a range of statutes, the operation and clarification of the different elements, and which is to take precedence,

---

29 See Caspar Bowden's submission to the Review. Similar concerns were raised by Open Rights Group, Liberty, Graham Smith and Peter Gill.

30 See Big Brother Watch's submission.

31 Reported, for example in "Plebgate: Met obtained phone records of Sun political editor without consent*",* the Guardian, 2 September 2014.

32 See "Sun makes official complaint over police use of Ripa against journalists, the Guardian website, 6 October 2014.

will need to be made clear. The current provisions of s80 (the general saving for lawful conduct) are, it is argued, opaque and complex.[33]

Scope of investigatory powers

12.32. Underlying the overwhelming majority of criticisms and submissions received from those in civil society was a fundamental concern regarding the scope and breadth of investigatory powers, although such a concern was not necessarily explicitly stated. While these concerns extended across the range of investigatory powers, two areas were of particular note: bulk collection of intercepted material and data retention.

12.33. There were a number of broad reasons for this. Many submissions were of the view that such bulk collection/retention could not (or, at the least, as currently practised in the UK does not) meet the requirements of the law, and in particular the requirements of EU law (articulated in *Digital Rights Ireland)* and the ECHR.[34] Others took a wider approach, highlighting alongside legal concerns the need for the protection of privacy as a social imperative,[35] and broader ideas regarding the type of society in which such collection/retention is permissible. The idea of "*sleepwalking into a surveillance society*", a concern first raised by the Information Commissioner in 2006, permeates some of these submissions. As stated by Open Rights Group:

> "… communications methods in general have expanded and the digital world makes surveillance even easier. The expansion of this approach means we have slipped into a mass surveillance model without a democratic debate regarding the consequences."

12.34. Unsurprisingly, given these concerns, the vast majority of those with whom I met from civil society emphasised the need for restrictions on those powers.[36]

Bulk collection

12.35. The idea of bulk collection of communications at the level of cables, with limited safeguards applied to such collection (rather than later access), is vehemently opposed by some of those who made submissions to me. Their reasons include the following:

(a) RIPA is, it is argued, is built on the idea of *targeted*, rather than *bulk*, warrantry (and therefore targeted surveillance and targeted collection). Bulk collection

---

33 In relation to interception, see further RIPA s1(5)(c), which provides that interception in relation to stored communications has "*lawful authority"* if undertaken under "*any statutory power"*. In relation to communications data, para 1.3 of the Acquisition Code states that public authorities should only use other powers if such powers explicitly provide for obtaining communications data. Section 21(1) appears to encompass within Chapter 2 any conduct for obtaining data (that falls outside of interception). DRIPA 2014 s1(6)(a) states that a service provider retaining communications data under DRIPA 2014 must not disclose it except under RIPA Part I Chapter 2, or as provided by regulations. See further Richard Greenhill's submission to the Review.

34 Including not only rights protected under Article 8, but also including rights to a fair trial, freedom of expression and freedom of association. These concerns are highlighted in the submission received from Dr. Paul Bernal.

35 As articulated comprehensively in the submission received from Dr. Paul Bernal, as well as in the submission of Charles Raab to the ISC.

36 Robin Simcox's submission was to the opposite effect.

represents therefore a "*qualitative change*" in surveillance,[37] with which the legal regime is ill-equipped to deal.

(b) Further, the lawfulness of bulk collection under the ECHR and EU law does not, it is argued, follow from the judgment in *Kennedy v UK*, which focused on the "*targeted*" 8(1) regime. The IPT has broadly upheld the legality of the s8(4) regime and bulk collection in the Liberty IPT Case (judgment of 5 December 2014), but many of those who made submissions to me are of the view that this will not prove the final word on the matter. It appears that the ECtHR will be called on to determine the issue in the application by Big Brother Watch and in the Liberty ECtHR Application. It was suggested to me, in advance of the IPT's judgment or with an eye to proceedings in Strasbourg, that:

- bulk collection is not "*in accordance with the law",* in particular because powers for bulk collection are not apparent from the face of the statute;[38]
- it is not proportionate, and indeed that it is simply impossible to have a meaningful assessment of proportionality at that level;[39] and that
- it does not provide adequately for certain material, such as material covered by LPP and material relating to journalists, which are considered below.

(c) The idea that collection is of itself an intrusion into privacy which requires careful justification (and, in law, a proportionality analysis) was consistently highlighted. Indeed, it was emphasised that whether or not a communication is *read*, the fact that it is collected is of itself an intrusion.[40] It was also stated that even if a person does not read or process the data, if there is technological processing of that data this is a further intrusion to mere collection.[41]

(d) There are concerns regarding the risk posed by holding so much data: it could be abused or accessed (unauthorised) by people outside the system.

(e) Fundamentally, there is a concern that such collection grants far more power to those conducting surveillance than is warranted, which undermines the basic balance between the citizen and the state. This has been done without public debate and proper scrutiny.

12.36. Some expressed the view that the alleged actions detailed in the Snowden Documents would, if true, be either unlawful or improper and should be prohibited (expressly, if necessary). Insofar as such actions are authorised by the current

37 See the submission of Dr. Paul Bernal.

38 As set out by the Equalities and Human Rights Commission.

39 See Global Network Initiative's submission

40 As set out in the submissions of Dr Paul Bernal and Professor Peter Sommer. This view is supported by the recent SURVEILLE Report, pp. 12-13.

41 As set out in submissions from Open Rights Group and the Bingham Centre for the Rule of Law. An example given of this point by Open Rights Group is the scanning of a person in a body scanner, rather than a personal examination by passport. One is technological, rather than human, but remains an intrusion into privacy.

regime, and in particular RIPA s8(4), the curtailment of such powers was urged, in a number of ways.

12.37. Some were of the view that only where a single person or premises can be identified would interception be appropriate. Another suggestion was that there should be a ceiling on the number of warrants that can be granted. Others have emphasised that s8(4) warrants must be detailed and specific (at least by purpose or geography),[42] such that there could not be a very small number covering a large proportion of internet traffic. Some have argued for the need for warrants set out by programme, such that individual warrants would cover particular operations run by intelligence or crime-fighting agencies, under which a range of targets would be covered. A further suggestion is to introduce a limiting requirement such as "*reasonable suspicion"* into the requirements for granting interception or collection of data.

12.38. A more common suggestion was for a shift in the legal framework (or, at the least, its interpretation), such that only targeted interception, rather than bulk or mass interception, is permitted.[43] In such a framework, a high threshold and robust safeguards attach to the first stage (the interception of data), rather than safeguarding only the access to or use of the information collected. This might entail the removal of the distinction between internal and external communications, discussed above.

12.39. The same, it is argued, should be true for collection of and access to communications data, such that obtaining such data is only possible in "*targeted*" situations. Moreover, in relation to obtaining communications data, some argue that the purposes set out in RIPA s22(2) are far too broad, and should be restricted, e.g. to "*serious crime"*.[44] A similar, although less common, suggestion is that fewer public authorities should have access to communications data, to ensure control over the scope of the powers.[45] However, others suggest that so long as the authorisation process and threshold are sufficiently robust, the specific body involved is less important.

12.40. One broad suggestion in relation to both interception and obtaining communications data was the adoption of a test that focused in particular on the nature and degree of intrusion, rather than the specific type of data, technology or authorising body involved.[46] This, it is suggested, would lead to a more nuanced proportionality assessment which would take better account of the interests and rights of the individual at stake, as well as future-proofing the system such that it would not be dependent upon types or definitions of technology or access.

12.41. For some, this would involve abolishing the distinction between content and communications data (discussed at 12.20 (b) and (c) above), such that there was a sliding scale of intrusion based on current categories: subscriber data, service use data, traffic data and content. There could be different levels of authorisation attaching to each, such that the lowest level (subscriber) could be self-authorised, and

42 See for example the submissions of the Guardian Media Group and Graham Smith.
43 See the submissions of Big Brother Watch, Open Rights Group and the Equality and Human Rights Commission.
44 See the definition in RIPA s81(2) and (3); and RIPA s5(3).
45 See for example the submission of the Bingham Centre on the Rule of Law.
46 See for example the submission of the Equalities and Human Rights Commission.

the highest level (content) judicially authorised. Alternatively, in line with suggestions of judicial authorisation set out in more detail below, different levels of judge could be called upon to authorise more intrusive data types. Others did not see "*intrusiveness*" as necessarily being linked to the type of data in question, but rather to a broader question of whether it would be intrusive to the target (which would take account of not only the data type but importantly also the degree of privacy attaching to the subject matter, and the steps taken to protect such privacy).

12.42. There were also calls to tighten up a number of the concepts within the authorisation regime to ensure intrusion only where necessary. In this vein, the need for a proper definition of "*national security"* as a legitimate purpose for interception or obtaining data was emphasised.[47] This, it was submitted, should be determined in public debate, and set out in clear guidance, rather than being purely for the executive to determine. Further, a few submissions emphasised that there must be clear guidance on what cannot be accessed or targeted, and is thus excluded from investigation altogether, such as for example lawful peaceful political activities.

Data retention

12.43. Similar concerns attach to the regime for data retention in the UK as attach to bulk collection, in particular in relation to the proportionality of the system. However, they are exacerbated by a commonly held view that the retention regime under DRIPA 2014 is unlawful, as it fails to take account of and/or undermines the CJEU's judgment in *Digital Rights Ireland*.[48] Liberty's view that "*mass communications data retention is undemocratic and unlawful"* is shared by other academics and NGOs. In particular, it is said to be disproportionate,[49] and entail insufficient limitations on its scale or scope.[50] That issue will soon come before the High Court.[51]

12.44. Other options are suggested. A number of submissions urged a regime of targeted retention, or "*preservation"* of metadata or communications data.[52] Under such a scheme, a dynamic list of suspects would have their data retained for certain specified periods of time (e.g. convicted offenders released on licence for offences for which recidivism is common). While there is a concern that this could stigmatise certain groups, or encourage profiling, those that espouse this view argue it is more proportionate than universal retention, as it focuses on a real and known threat. There are even narrower suggestions, which do not fall foul of such considerations, including a retention order for specific individuals named in the order based on a specific investigation or proceedings.[53] In response to the suggestion that this would only deal with known threats, there is a further suggestion of a "*centre of analysis*" which would be able to investigate links and generate new targets. Arising across some of these more targeted suggestions is a view that this targeting should be authorised by judges on a case-by-case basis, targeted at those "*reasonably believed"* to be engaged in

47 See the Open Rights Group submission.
48 This was set out in the submissions of the Law Society and Access.
49 See the Equalities and Human Rights Commission.
50 See the Center for Democracy & Technology.
51 *R (David Davis MP and Tom Watson MP) v Secretary of State for the Home Department* CO/3794/2014, not yet heard.
52 See Professor Peter Sommer, Caspar Bowden, Center for Democracy & Technology.
53 See the Center for Democracy & Technology.

criminal activities, and with notification of the target where preservation has been wrongly undertaken.

Hacking, CNE and encryption standards

12.45. As set out above, there are concerns in civil society regarding (in particular) the recently acknowledged use of CNE, the allegation in the Snowden Documents that public authorities are seeking to break encryption standards, and the alleged use of a range of methods for surveillance not set out explicitly in law.[54] As well as the concern I have already mentioned, regarding the basis for such powers in law, there are significant concerns regarding the use of these methods at all. In particular in relation to encryption, some are of the view that these methods are dangerous for the safety and security of the users of the internet. Moreover, CNE presents a dizzying array of possibilities to the security and intelligence agencies, and while some methods of CNE may be appropriate, many are of the view that there are others which are so intrusive that they would require exceptional safeguards for their use to be legal. The use of CNE by the security and intelligence agencies is one of a number of issues in the PI IPT Case.

Increase scrutiny and safeguards

Increase scrutiny

12.46. As set out in Chapter 6, in the vast majority of cases the scrutiny that takes place prior to authorisation being granted is undertaken either internally by the body concerned or by the Secretary of State. This has been the subject of considerable criticism. Most in civil society are of the view that this is simply insufficient to guarantee protection for fundamental rights and civil liberties.

12.47. For interception, which is authorised by the Secretary of State or Scottish Minister:

(a) The primary concern is that the Secretary of State's position means that it is difficult, as the head of the relevant institution, to take a robust and independent judgment as to the proportionality of each request. This is not an attack on the capability or independence of any particular Secretary of State, but rather upon the institutional nature of the position. It is magnified by a position where refusal of warrants is rare,[55] and oversight is not considered robust (as described below).

(b) It is difficult to reconcile with the doctrine of the separation of powers (whereby the executive, parliament and judiciary remain separate), and has been argued as being constitutionally inappropriate as it grants the executive too much power.

54 Highlighted in particular by Access and Privacy International.

55 See the *Report of the IOCC for 2003,* para 8, *Report of the IOCC for 2009,* para 2.3 and *Report of the IOCC for 2010*, para 2.4.

(c) It places a heavy burden on a small number of politicians. Of particular concern is the time and level of scrutiny that can be granted to each warrant in those circumstances.

(d) There is limited explicit provision for when the relevant Secretary of State is unavailable.

(e) In relation to the argument that the Secretary of State brings democratic legitimacy to the process, it is contended that democratic legitimacy is limited, both in practice and in principle: there are limits to the efficacy of democratic accountability in any event, and certainly in an area in which public mood can be greatly swayed by particular incidents and in which minorities may be likely to be targeted.

12.48. Related issues arise as far as communications data is concerned, and in particular those raised as points a) and b) above. The lack of institutional independence is clear: for the acquisition of such data, pursuant to RIPA s22,[56] each body able to request such data has a DP who can request service providers to provide it. There is judicial approval only of authorisations granted or notices issued by local authorities (s23A). In these circumstances, while the Codes of Practice set out the responsibilities of those involved, without external input there is a concern that the robustness of the mechanisms is dependent at least in part on the personalities or corporate culture of those involved. Moreover, within certain public authorities trust may have been eroded by their use of powers without safeguards (such as alleged police use of RIPA Part I Chapter 2 to determine journalistic sources).

12.49. In light of the above, some have advocated for a centralised expert decision-making body responsible for the authorisation of surveillance. This could, it is suggested, entail different levels of decision-maker so that individual decisions regarding low-level intrusion could be dealt with separately to broader and more intrusive powers.

12.50. However, by far the most common suggestion emphasised in this regard was the increased use of judicial authorisation for authorising surveillance (both before interception and prior to obtaining or disclosing communications data).[57] Submissions highlighted that this has been an approach preferred by a number of oversight bodies, including the House of Lord Constitution Committee,[58] and the Joint Committee on Human Rights.[59] It was said to be preferable for a number of reasons:

(a) It would be more likely to satisfy the standards of human rights law set out in particular in *Digital Rights Ireland* (of prior review by a court, at para 62) and also the judgments of the ECHR, detailed in Chapter 5.

---

56 And often other regimes, set out in Chapter 6.

57 Such submissions were received, for example, from Big Brother Watch, Professor Peter Sommer, Open Rights Group, the Equality and Human Rights Commission, Liberty and the Bingham Centre for the Rule of Law. An unusual example of a submission where this was not advocated is the thoughtful submission I received from students at UCL.

58 *Surveillance: Citizens and the State,* (2009), HL Paper 18-1, para 163.

59 *Counter-Terrorism and Human Rights: 28 Days, Intercept and post Charge Questioning,* HL 157/HC 394 (July 2007), para 161.

(b) It would bring more independence and thus trust to the decision-making procedure.

(c) It would be entirely workable.

12.51. It is a model that has been successful in other countries,[60] and that operates in relation to other investigatory powers in the UK. For many, it is clearly the appropriate level of scrutiny required to authorise the type of intrusion in question: as English law has long recognised the need for a judicial warrant for the search of a person's home, the equivalent should be required to access the information available regarding a person based on their communications (which may be very intrusive and informative).

12.52. Modifications of this broad suggestion included the suggestion of judicial scrutiny alongside ministerial scrutiny,[61] or judicial authorisation for certain activities or certain data, or the use of a model of a Commissioner.[62] In response to considerations of urgency raised by public authorities, suggestions noted that there could be provisions for *ex parte* out-of-hours requests that could be dealt with extremely quickly, as well as the possibility of a short (24 or 48) hour period in which urgent authorisations were permitted internally and then had to be reviewed and authorised by a judge at a later stage.[63]

12.53. As set out further below, the need for such authorisation is particularly emphasised in relation to the content and communications data regarding or revealing journalistic sources[64] or that which is covered by LPP.

12.54. However, there is a general view that judicial authorisation by magistrates of local authority applications pursuant to ss23A and 23B has not been an effective means of securing more robust scrutiny.[65] Thus, in line with these criticisms, most of the submissions on this point did not suggest granting further decision-making powers to magistrates but rather to transfer such powers to the High Court or a similar level. Indeed, judicial authorisation is not, as others have pointed out, a "*panacea*".[66] It does not (necessarily) provide for oversight "*downstream*", i.e. after-the-event scrutiny. However, as has been emphasised to me, it may provide further independence, greater scrutiny and increased public trust.

---

60 According to the submission I received from Liberty, who pointed to the United States of America, Australia, Canada and New Zealand as examples: see further 8.40 above and Annex 15 to this Report. See also the UN Office on Drugs on Crime, *Current practices in electronic surveillance in the investigation of serious and organised crime*, (2009), p. 17.

61 See Dr Andrew Defty and Professor Hugh Bochel. This would be a system similar to that existing in Canada, as set out further in Annex 15 to this Report.

62 As set out in the submission of the Bingham Centre for the Rule of Law.

63 See the submission of the Guardian Media Group.

64 As indeed was recognised in IOCCO's *2015 inquiry into the use of Chapter 2 of Part 1 of RIPA to identify journalistic sources*, (February 2015).

65 See the *2013 Annual Report of the Chief Surveillance Commissioner*, para 3.10; IOCCO's submission to this Review, 3.11.12-15.

66 See IOCCO's submission to this Review, section 3, and *IOCC Report*, (March 2015), paras 6.54-6.59 and 7.36-7.39.

Increase safeguards on access to and use of data

12.55. Safeguards are not only necessary when collecting, acquiring or accessing data. They must also be available, and be robust, at later stages, and in particular as regards the use of such data, especially as this will be a further intrusion under Article 8 of the ECHR. However, a number of submissions emphasised to me that the protections currently set out in RIPA ss15, 16, 22 and 23 and the Codes of Practice are insufficient for this purpose. Possible ways to improve the current position were set out.

12.56. First, it was argued that safeguards should extend more widely, including to material accessed under DRIPA 2014, to communications data under RIPA Part I Chapter 2 (as to which there are limited safeguards), and to interception or obtaining of data outside the RIPA regime.

12.57. Secondly, safeguards must be more explicit and more stringent. Thus submissions urged:

(a) clear authorised methods for searching data,[67] perhaps including published terms;

(b) special authorisation for search terms that are particularly intrusive;

(c) narrowing the constraints on the *use* of such data, such that it can only be *used* in line with the purposes for which it is *collected*, or require later authorisation;

(d) granular and explicit purposes for which it may be used (rather than broad terms such as "*national security"*);

(e) only permitting the authority that accessed the data to then use it, or requiring further authorisation for it to be transferred;

(f) the review of data at regular intervals for destruction; and

(g) robust and clearly defined rules for the destruction of intercepted material, including time limits.

12.58. Two particular ways of ensuring this have been highlighted. Strict rules on data minimisation (i.e. the holding of the "*minimum*" amount of data necessary) could be implemented, similar to the controls imposed by the FISC in the United States relating to information concerning United States persons (see Annex 15 to this Report). Alternatively, the possible utility of ordinary data protection principles being applied across the board was also emphasised.

12.59. The concerns regarding safeguards on the use of information apply broadly across investigatory powers, and are not confined to access to data. Thus, it is urged that, for example, there should be "*Chinese walls*" between those developing cryptographic

[67] See for an example of this, *Report of the CTIVD in the Netherlands on the processing of telecommunications data*, (February 2014), p. 15 et seq.

standards and those empowered with the mandate to uncover threats to national security.

Provide for special protection

12.60. A "*one-size-fits-all*" approach to intrusion into personal affairs is, it is argued, both unsatisfactory and potentially unlawful. I received a number of submissions on the subjects of sensitive information, particularly in relation to data that could reveal the source of journalistic information;[68] data protected by LPP; or information that is deeply personal and private, such as medical records. In light of the important safeguards required in particular by the ECHR (see 5.44-5.53 above), a number of those with whom I spoke were of the view that insufficient guidance is found on these important topics either in RIPA itself or in the Codes of Practice (in contrast to the heightened scrutiny clearly set out on the face of other legislation, including PACE ss9-14 and the Police Act 1997 ss97-100). This is a topic on which there have been updates during the course of the Review, which may meet some of these criticisms.

12.61. Taking ***journalistic material*** first, the starting point is that set out by Liberty: "*[a] free press and the right to free speech is dependent on respect for private correspondence"*. By allowing public authorities to discover the source of journalistic material (without clear safeguards), this important principle is said to be undermined. This was of pivotal importance to some of the submissions I received, including from Gavin Millar QC, the Newspaper Society, the Media Lawyers' Association, the National Union of Journalists and the Society of Editors. These submissions highlighted the following important considerations:

(a) Article 10 of the ECHR and judgments of the ECtHR, set out in Chapter 5, require scrutiny of decisions to access material in relation to journalist's sources.

(b) Communications data is particularly relevant, as the content of the communication is often publicly available.

(c) As other regimes protect this area, RIPA may "*undermine"* those safeguards.

12.62. Changes were urged to the current scheme, in particular to "*safeguard the media's role as a public watchdog, which forms one of the cornerstones of a democratic society*".[69] In particular, submissions highlighted the possible need for: i) judicial scrutiny;[70] ii) further requirements in the Codes of Practice;[71] or iii) some manner of "*shield law"* to protect sources.[72]

12.63. The use of RIPA to collect material on sources was widely publicised in relation to the "*plebgate*" and Chris Huhne affairs.[73] Popular opinion surveys demonstrated support

68 See the submission from the Newspaper Society.
69 Media Lawyers' Association, Newspaper Society.
70 See the submission of the Media Lawyers' Association.
71 *Ibid*.
72 Submission of Gavin Millar QC.
73 For a detailed discussion of these points see *IOCCO inquiry into the use of RIPA Part I Chapter 2 to identify journalistic sources,* (February 2015),.

for restrictions on police access to phone records.[74] This led IOCCO to consider this area in late 2014-2015, and to recommend judicial authorisation for the police accessing communications data for the purposes of "*determining*" a source, but finding that otherwise ordinary procedures can be used (with bolstered guidance in the Code of Practice).[75] As emphasised by Jan Clements to me, any consideration of this issue requires care and safeguards not only in relation to the identification of a source, but also in relation to the fact that a source has been in touch, and in relation to the location, timing and frequency of communications.

12.64. Some of these criticisms may have been addressed by the (very) recent changes to the framework for such data. The Serious Crime Act 2015 s83 inserted into RIPA s71 a requirement for a code of practice which "*shall include provision designed to protect the public interest in the confidentiality of journalistic sources*". The Draft Interception Code requires "*particular consideration"* to be given to such material.[76] The new Acquisition Code notes that interference with privacy may be higher in such situations, requires a record to be kept, requires "*particular care"* over applications for such data, and requires law enforcement to use PACE provisions to seek a production order when they wish to identify a journalist's source.[77]

12.65. The importance of ***LPP*** was highlighted by the Bar Council, which noted that it forms the *cornerstone of a society governed by the rule of law"*. Some submissions focused almost exclusively on this issue (including those of the Bar Council and the Faculty of Advocates). These submissions have been partially validated by the admission by the government in the Belhadj IPT Case that its procedures for dealing with LPP material were in violation of the standards required by Article 8.[78] The question then becomes what is in fact lawful. One particular issue concerns whether or not communications data may attract privilege. While this was not the focus of the submissions I received, the new Acquisition Code makes clear the Government's view that it cannot, at para 3.72. As explained at paras 5.45-5.46 above, the contrary is certainly arguable where the communications data discloses not just the existence of the lawyer-client relationship but also the substance of the advice sought and given (for example the identity of an expert witness who has been cc'd into an email). In the context of interception, and in particular in cases against the Government it is emphasised that there must be robust barriers between those collecting data and those involved with the cases in question. It is broadly accepted that extra safeguards would not apply to cases in which LPP is used to further a criminal purpose.

12.66. Again, as with journalistic sources, there have been recent amendments to the Code of Practice which entail further safeguards. In the new Acquisition Code, while there is no specific requirement for applications (as there is in relation to journalistic

74 Polling was conduct by Ipsos MORI for the Evening Standard in October 2014. See "Public backs curbs on police seeing phone records of journalists", London Evening Standard, 21 October 2014.

75 *IOCCO inquiry into the use of RIPA Part I Chapter 2 to identify journalistic sources,* (February 2015), para 8.9.

76 Draft Interception Code, para 4.19.

77 Paras 3.73-3.84.

78 See the Order of the Court handed down on 26 February 2015

sources), "*special consideration"* must be given to necessity and proportionality, and a record must be kept.[79] The Draft Interception Code is more detailed.[80]

12.67. Suggestions were posed in relation to both LPP and journalistic sources, including:

(a) Adopting a similar scheme to that set out in PACE, such that police must have an application to a circuit judge under Schedule 1 approved before they can access personal records, journalistic material, and items subject to LPP. Similarly, under the Police Act 1997, a Commissioner appointed pursuant to s91 (rather than the ordinary authorising officer) must authorise property interference where it is likely to result in the acquisition of knowledge of LPP matters, confidential personal information or confidential journalistic information. In the case of communications data which may lead to the identification of journalistic sources, as set out above, this has already been implemented.

(b) A bar on targeting information of this nature (although not necessarily a bar on use), or a bar on targeting without a warrant issued by an oversight body.

(c) Mandatory reporting to an oversight body where confidential or journalistic source material is identified, or indeed where there is a reasonable belief that the intrusion may give rise to data of this nature, which then could be assessed pursuant to a stringent proportionality test and the requirements of Articles 8 and 10 (set out in detail in Chapter 5).

Provide for robust sanctions

12.68. A few suggestions I received highlighted what is perceived to be minimal accountability for what can appear to be very serious breaches of the law. Serious intrusion into privacy has been undertaken (perhaps the "*most visceral illustration"* of which, according to Liberty, is the alleged OPTIC NERVE program: see Annex 7 to this Report). Yet in relation to much of the allegations in the Snowden leaks and the findings of unlawfulness in the IPT, no public sanctions appear to have been imposed. This is in part due to the minimal sanctions in the statutory regime:

(a) According to RIPA s72(2), failure to comply with the Codes of Practice by any person "*shall not of itself render him liable to any criminal or civil proceedings"*.

(b) While s22 states that it is "*lawful*" to obtain and disclose communications data if it is done under RIPA Part I Chapter 2, or to do that which is incidental to that conduct (s22(3)), there is no clear sanction for a breach of the communications data provisions.

(c) This confusion is exacerbated by RIPA s80, which provides that conduct which is not otherwise unlawful under RIPA or would not be unlawful apart from RIPA is lawful.

79 Paras 3.73-3.75.
80 Draft Interception Code, paras 4.4-4.18.

(d) Further concerns are raised regarding the limits of sanctions imposed on service providers by DRIPA 2014,[81] which do not impose a specific offence for unlawful disclosure of data collected under that statute.

12.69. Yet robust and clear accountability and sanctions for breaches of standards is necessary, it is argued, to ensure compliance.[82] One way of achieving this might be the admissibility of intercept evidence into court.[83]

12.70. Moreover, many civil society actors were of the view that there should be enhanced protection for whistleblowers, including a clearer route to oversight mechanisms and fewer sanctions.

Data sharing and seeking data from abroad

12.71. The failure to regulate for and provide safeguards as to data sharing with other states has not only been criticised,[84] but in certain circumstances has been found unlawful.[85] While in the Liberty IPT Case it was broadly found that current practices in relation to the receipt of information from abroad, are now lawful, mirroring the conclusions of the ISC in relation to PRISM,[86] this is a matter which is further raised in Big Brother Watch's application and in the Liberty ECtHR Application. No similar decision has been undertaken in relation to the receipt of communications data from overseas. Even if current standards can be said to satisfy Article 8, many in civil society are of the view that the safeguards applying should be set out in law and significantly more robust. In particular, as most states apply differential safeguards based on citizenship and/or geography (with heightened safeguards being required closer to home), the weaker standard will become the norm if extensive and unregulated data sharing is undertaken. It was emphasised that it should be unlawful to obtain data on UK citizens from foreign governments that it would be unlawful to obtain within the UK, and that sanctions should attach to these obligations. There is also a need for clear standards on the *use* and *access* to data from foreign sources.

12.72. Likewise, there were concerns not only in relation to the receipt of data from other states but also the sharing of data by UK authorities.[87] The UKUSA Agreement sets out the basis for data sharing in only the most general terms. As explained in Chapter 6, the Secretary of State exercises a very broad discretion when determining whether data should be shared with a foreign State. It was argued that this sphere was insufficiently regulated, particularly in relation to data sharing amongst the Five Eyes. There is nothing in the public domain concerning the guarantees secured by the UK Government concerning the storage, retention, destruction and use of those data.

81 Data Retention Regulations 2014/2042, see in particular regulations 12(2), 13(2)(b) and 15(9).
82 Richard Greenhill's submission dealt with the lack of sanctions for a range of issues.
83 As urged in particular by the Guardian Media Group and the Bingham Centre for the Rule of Law.
84 As it was, heavily, in the submissions received from in particular Access, as well as the All Party Parliamentary Group on Drones.
85 In the Liberty IPT Case, described in more detail in Chapter
86 Liberty IPT case, judgment of 5 December 2014; ISC, *Statement on GCHQ's alleged interception under PRISM,* (July 2013).
87 As helpfully set out in the submission from the All Party Parliamentary Group on Drones.

Clear guidance should, it was urged, be provided for these processes, as well as accompanying oversight mechanisms.

12.73. A related topic is the extraterritoriality provisions in DRIPA 2014, considered in a number of submissions I received.[88] These focused on the legal complexities of requiring companies in other states to comply with notices and warrants issued in the UK, as well as on practical concerns regarding the enforceability of such practices. During the course of this Review, these issues have become more prominent.

12.74. In relation to the above criticisms, and recognising the need for information from service providers outside the country, the focus of these submissions was often on the development of MLATs.[89] This, it is suggested, would be clearer, avoid extra-territoriality concerns, and be more likely to satisfy the conditions of the law. Insofar as there are criticisms that MLATs are slow or ineffectual, those with whom I spoke considered that the focus should be rather on improving and securing access through them rather than finding ways around them.

12.75. Some placed their faith in an international agreement or on international law to ensure cooperation in data sharing.[90] However others recognised that while a UN Convention or an additional international treaty would be of assistance in regulating international data sharing, it was both an unlikely event and perhaps unlikely to operate effectively in the face of alliances and hostilities between states.

Improve oversight

12.76. The oversight mechanisms for investigatory powers received significant criticism in a high proportion of the submissions I received. Suggestions were made both to individual oversight mechanisms and to the oversight regime as a whole,[91] which was described by Human Rights Watch as "*neither transparent nor comprehensive"*.

12.77. Broadly, the submissions I received demonstrated limited trust in the oversight mechanisms. Several pointed to the attitude to oversight apparent from the Snowden Documents: in particular that legal advisers had made a note to tell the NSA "*[w]e have a light oversight regime compared to the US*"; [92] that the regulatory regime was a "*selling point*";[93] and that the legality of OPTIC NERVE "*would be considered once it had been developed*".[94] Many thought that the revelations in the last few years, including but not limited to those contained in the Snowden Documents, should have been highlighted much earlier by oversight mechanisms.[95]

88 Including those from Graham Smith, the Center for Democracy & Technology, Liberty, and the Global Network Initiative.

89 Including Graham Smith, Center for Democracy & Technology and Global Network Initiative.

90 As set out in M. H. Halperin et al, "Multilateral Standards for Electronic Surveillance for Intelligence Gathering", (January 2015), Oxford Internet Institute Discussion paper.

91 Some submissions, such as those by Dr Andrew Defty and Professor Hugh Bochel, focused almost entirely on oversight.

92 "The legal loopholes that allow GCHQ to spy on the world", The Guardian website, 21 June 2013.

93 "NSA pays £100m in secret funding for GCHQ", The Guardian website, 1 August 2013.

94 "Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ", The Guardian website, 28 February 2014.

95 As set out by Peter Gill, the "*mass trawling"* undertaken by GCHQ should have been set out in the reports of IOCCO.

12.78. While I set out these criticisms below, it is fair to recognise that the oversight bodies themselves, whose views are not included in a separate Chapter, have engaged constructively with me over the course of the Review. I have taken those positions, and helpful discussions, into account in considering the force of the criticisms below. Furthermore, the oversight mechanisms have achieved more public prominence in the last year, and in particular after the main deadline for written submissions to the Review. Some of the criticisms of oversight may have receded in the light of recent detailed reports of the IOCC and ISC, and two IPT judgments finding against the security and intelligence agencies.

Overarching considerations

12.79. A number of submissions to this Review emphasised the confusing array of individual oversight mechanisms, with little clarity as to the demarcation between them. Simplifying this oversight and ensuring that insofar as different bodies were involved they worked as a cohesive unit was thus a key feature of a number of suggestions.[96] Many highlighted the need for better coordination amongst all oversight bodies, and particularly the ISC and the IPT, including the need to ensure access to confidential annexes to the reports of other bodies. Moreover, a clear framework of responsibility, by function or body, and a hierarchy of responsibility, would, it was suggested, increase efficacy. Further, oversight bodies must have access to other systems: it should be possible for the oversight body to easily pass on complaints to prosecutors or Parliament.

12.80. Others have gone further to suggest the need for a single, full-time, independent expert body (a "*super-regulator*") with responsibility for all the different elements of oversight.[97] Were all surveillance powers to be brought together, this body would therefore be responsible for all surveillance (including that which falls outside the focus of this Review). Such an oversight body, in some submissions termed an "*Inspector General*", in others a general "*Surveillance Commissioner*", would need to be well resourced.

12.81. This was thought to have the significant benefit of simplifying oversight and assisting with the consideration of proportionality. But there was concern particularly from the ISCommr about diluting the personal responsibility of the current Commissioners, and it was suggested that running a super-regulator could be too big a job for a retired judge who wished to work only part-time.

12.82. In any event, in considering how to develop cohesive bodies, many emphasised the need for oversight by technical specialists. This could either be done by providing well-resourced assistance from technical and legal experts, or the increased use of technical experts as part of the oversight mechanisms themselves (rather than in simply supporting roles). A broader suggestion would encompass the use of "*panels*" with officials from both a national security background and those who have expertise in the protection of civil liberties from an external perspective. DEMOS suggested

96 See the submission of Peter Gill.

97 As set out in the submissions I received from the Equality and Human Rights Commission, the Bingham Centre for the Rule of Law, and students at UCL.

that the oversight (or warranting) process would benefit from the use of "*surveillance juries*". As the jury is a trusted institution, it was thought possible that it could secure further public trust (particularly if supported by other oversight bodies and an expert technical secretariat).

12.83. Broadly, submissions emphasised the need for a *proactive* rather than *reactive* regulator/oversight body, with sufficient resources, sufficient investigatory expertise and sufficient powers to be able to actively hold public authorities to account. Moreover, the oversight body must have a public-facing profile to secure public trust and ensure that public complaints can be considered.

Gaps in oversight

12.84. A number of gaps in the scrutiny and oversight mechanisms were highlighted to me,[98] including:

(a) the use of the wide range of powers to acquire stored communications data other than by way of RIPA Part I Chapter 2 (for example the use of PACE s9 orders);

(b) the use of TA s94, which the IOCC has recently been asked by the Prime Minister to oversee;[99]

(c) the implementation of DRIPA 2014 s1 and means of redress for a service provider who believes that a notice has become disproportionate (and their request for cancellation has been refused);

(d) interception of stored communications where a statutory power or production order is used;

(e) procedures and requirements for data sharing (which is currently only partly considered by the ISC and the Information Commissioner);[100] and

(f) errors on the disclosure side, and particularly wrongful disclosures or failure to disclose by service providers.

12.85. Finally, the statutorily required Northern Ireland Commissioner (RIPA s61) does not exist.[101] Thus, it is submitted that these gaps must be closed (potentially by the use of a single regulator, as set out above). A related concern is the concern that, at times, the different scrutiny mechanisms may overlap. While "*more*" scrutiny might be seen as better than "*less*", this leads to several problems, including inconsistency of results and confusion as to the correct outcome. Again, it is argued that this could be achieved by the use of a single regulator.

98 In particular by IOCCO's submission to the Review.
99 *IOCC Report*, March 2015, section 10.
100 As highlighted by Peter Gill.
101 As highlighted by Paul Connolly.

Commissioners

12.86. The system of Commissioners came in for considerable criticism from civil society. Concerns ranged from those regarding the Commissioner system and structure, to those specifically based on the operation of the Commissioners within that structure:

(a) The wide range of Commissioners was argued to be inaccessible and confusing, notwithstanding initiatives such as the Surveillance Road Map,[102] meaning that oversight depends on very fine distinctions.

(b) The fractured nature of the Commissioners' work means that they are argued to be ill-placed to assess the proportionality of measures undertaken.

(c) As judges, suited well to adversarial disputes, their suitability for an inquisitorial role has been questioned, and the potential need for technological expertise highlighted.

(d) Commissioners are appointed by the Prime Minister, but to ensure freedom from executive influence would be better appointed by Parliament directly.

(e) There is a lack of public knowledge of and interaction with the Commissioners, which is at least partly based on the lack of public-facing efforts by Commissioners (although it is recognised that this criticism may increasingly not apply to IOCCO, and developments in this regard were encouraged).

(f) The extent of scrutiny is inadequate, in particular:

- the percentage of warrants considered is argued to be insufficient (although it is recognised that IOCCO has increased the warrants it inspects), with many suggesting that Commissioners should look at far more (perhaps even all warrants);

- the reports written by the Commissioners are insufficiently probing, being described as "*formulaic and superficial"* until 2013, and, in relation to the more detailed reports appearing thereafter (which are not universal), "*cheerleading with caveats"* thereafter; such that many urged the need to continue less "*bland"* reports in future, ensuring that the detail allows for public scrutiny;

- in functioning as audit mechanisms (as they were intended by Parliament), the Commissioners are not well placed to bring to light serious and systematic intrusions into privacy, and there is a view amongst civil society that the Commissioners should have highlighted practices which are now public, and which have since been examined by the IPT.

[102] Produced by the ICO, IOCCO, the ISCommr, the IPT, the OSC, the Office of the Biometrics Commissioner, and the Surveillance Camera Commissioner, (August 2014).

(g) Commissioners have only recently begun to deal with inquiries and reports into alleged abuses, which form a vital part of effective oversight.

(h) Commissioners, particularly the ISCommr, are inadequately resourced, and should be bolstered with better resourcing, full-time operation, and greater powers to call for evidence and question national security bodies.

12.87. A common suggestion regarding the above was that the functions of different Commissioners should be merged, or at the very least their interaction should be clarified. In particular, in relation to the latter point, Commissioners should be divided either by the acts/functions of the public authorities in question (i.e. interception, acquisition of communications data, targeted surveillance, etc) or by the bodies in question (e.g. agencies, police, other public authorities), to avoid confusion.

Investigatory Powers Tribunal

12.88. During the course of the Review, the IPT had before it a number of major cases, arising out of the Snowden documents and operations in Libya. It ruled for the first time that the security and intelligence agencies had acted unlawfully (albeit only in the past, and in a relatively technical respect), and appears to have been the catalyst for significant disclosures and concessions by the Agencies. A respected commentator wrote recently of *"the reputation [it] is slowly building for itself"*.[103] While the voices calling for its abolition appear muted, criticisms of the IPT remain, again regarding both the institutional mechanisms and its operation.[104] Some complained to me that:

(a) The percentage of complaints upheld is very low[105] in comparison to other similar bodies.

(b) It has insufficient technological expertise.

(c) It is insufficiently transparent:

- Most decisions are uninformative, and reached without a hearing;
- Similarly, ordinarily no reasons are given for the refusal of cases;[106]
- Without consent the Tribunal cannot even disclose the fact of a closed hearing (see rules 9(4) and 6(2)-(3));
- It cannot compel oral evidence at a hearing;
- It must ensure that information is not disclosed if this would be contrary to *inter alia*, the public interest, the economic well-being of the UK or the

103 J. Rozenberg, "Legal privilege and the conflicting interests of GCHQ and the IPT", the Guardian website, 16 March 2015.

104 Further detail of some of these criticisms is provided by Open Rights Group and Liberty.

105 From the IPT website, *Operation – Cases Upheld*, http://www.ipt-uk.com/section.aspx?pageid=9.

106 See the IPT website, *Operation- Determinations and non-determinations,* http://www.ipt-uk.com/section.aspx?pageid=11.

continued discharge of the functions of the intelligence services (rule 6(1)), although "*gists"* of evidence are now permitted;[107] and

- It operates based on the principle of NCND,[108] a "*departure from procedural norms*".[109]

(d) There is no appeal from the IPT (RIPA s67(8)); nor does it appear that the IPT can make declarations of incompatibility under HRA 1998.

12.89. A range of suggestions seek to address the criticisms made of the IPT itself, and include:

(a) The grant of greater powers to the IPT:

- to allow it to issue a "*declaration of incompatibility*" (as far as this is not provided for currently);
- relating to disclosure;
- to extend the use of oral hearings;
- to make open hearings the default and disclose the fact that closed hearings have taken place;
- to use special advocates so as to ensure a degree of representation for the interests of those excluded from closed hearings; and
- to secure further and more robust powers for ordering disclosure, including sanctions where information is not provided.

(b) Increasing the capability of the IPT, including the introduction of expert technological expertise.

(c) Expanding the scope of the IPT's jurisdiction to allow it to consider errors made by service providers as well as public authorities.

(d) The ability for further scrutiny of the IPT's work, including in particular the introduction of judicial review and/or appeal of IPT decisions.

(e) Measures to increase access to the IPT, including:

- giving more bodies the ability to refer issues to the IPT, including service providers and other oversight mechanisms such as Commissioners;

---

107 The Belhadj IPT Case, interim judgment of 18 November 2014.

108 See the discussions in IPT/03/03/CH, *Kennedy v Security Services* IPT/01/62 and 77 (in particular paras 46-54), and the Belhadj IPT Case.

109 *Secretary of State for the Home Department v Mohamed and others,* [2014] EWCA Civ 559, [2014] 1 WLR 4240.

- providing for notification of those wrongfully subjected to investigatory powers (unless an operational need requires otherwise); and

- granting legal aid to claimants and the ability to award costs to ensure that those with limited means are able to access justice.

(f) Measures to ensure greater transparency, which include:

- increased fact-finding power, including lessened reliance on the NCND principle where public interest demands otherwise;

- the increased giving of reasons for refusing cases; and

- the production of greater public information regarding the operation of the tribunal.

Intelligence and Security Committee

12.90. The ISC was reformed by the JSA 2013. However, concerns remain that the ISC is insufficiently robust and independent of governmental pressure. In particular:

(a) Its members still require nomination by the Prime Minister.[110]

(b) It may not consider matters that the Prime Minister views as either not in the significant national interest or part of an ongoing operation.[111]

(c) It must exclude matters that the Prime Minister considers would be prejudicial to the continued operations of the intelligence services.[112]

(d) Information can be withheld from it by the Secretary of State if such information is "*sensitive*" (i.e. leading to identification of or providing details of sources, assistance or operational methods available to intelligence or security bodies) or should not be disclosed in the interests of national security.[113]

12.91. Submissions focused on bolstering the powers given to the ISC, such that it could compel the production of information, hold more (and more robust) public evidence sessions,[114] and perhaps look more broadly at the acts of the security and intelligence agencies. This would require more funding and more staff. Other suggestions included providing the ISC with independent experts able to undertake detailed forensic investigations and an independent secretariat with both legal and technical advisors.

110 Section 1(4)(a).
111 Section 2(3)(a).
112 Section 3(4).
113 Schedule 1, para 4(2)-(5).
114 Recent hearings were described as *"political theatre"* by Dr Paul Bernal.

12.92. Some submissions focused on the independence (and further the perceived independence) and institutional security of the ISC, which it was thought could be improved by:

(a) ensuring that key members of the committee have not had dealings with or political responsibility for the intelligence services;

(b) the chair of the ISC being a member of the Opposition;

(c) a transparent selection process not limited to nominations by the Prime Minister, perhaps by way of appointment by Parliament or Select Committee;

(d) reporting directly to Parliament rather than placing reports first before the Prime Minister; and

(e) making its own decisions on reporting and publication, removing the automatic veto by the Prime Ministers. In sum, this may entail the ISC becoming a full Parliamentary Select Committee.[115]

12.93. It is fair to point out that the deadline for written submissions to the Review came before the publication of two weighty reports, which may have gone some way towards rescuing the reputation of the ISC.[116] However the ISC as an institution did not receive significant support from those making submissions to us. Some were even of the view that it should be abolished and its functions transferred to other Parliamentary Committees such as the Joint Committee on Human Rights and the Home Affairs Committee.

Future-proofing

12.94. The difficulty of predicting the direction and nature of technological development underlies many of the criticisms of the current regime. A framework designed in 2000 does not, it is argued, stand up to analysis in 2015. It is difficult to describe accurately the vast technological changes that have occurred in that time: but by way of example we transmit vast quantities of data about the most mundane elements of our daily lives across multiple borders in seconds; computers and handsets can be remotely accessed and controlled without a suspect even being aware of it; and at any point in time when we are carrying a mobile phone our location can be pinpointed with significant accuracy.[117]

12.95. The advantages of future-proofing (and its regular companion phrase, technological neutrality) have been emphasised to me countless times. At its root is a concern not only that the law will become unusable, but that public authorities (and in particular the Agencies) will develop capabilities that appear justifiable on an existing legal framework but as to which safeguards are of minimal impact.

---

115 For detailed discussion of the role of and potential improvements to the ISC, see the submissions of Big Brother Watch, ORG, the Bingham Centre for the Rule of Law and Dr Andrew Defty and Professor Hugh Bochel.

116 The ISC Rigby Report and the ISC Privacy and Security Report.

117 See further Chapter 4, above.

12.96. Future-proofing is far from easy, although suggestions include:

(a) a statutory requirement to review the law at regular intervals;

(b) sunset clauses in legislation (in which the legislation expires following a certain period, as in the case of DRIPA 2014);

(c) a requirement to publish up-to-date and detailed Codes of Practice at regular intervals; and

(d) the grant of specific powers and the outlawing of other powers such that for any further powers to be exercised they have to be specifically authorised.

12.97. Some placed their faith in the parliamentary system to ensure future-proofing. One suggestion was to develop standing committees to review (all) Acts of Parliament to ensure that they are technologically relevant and robust, or likewise to review all security measures to ensure compliance with human rights law. Similarly, the Information Commissioner has himself noted that when passing legislation which impinges on privacy norms that there should be published a privacy impact assessment, or Commissioners should be permitted to publish a report.[118] He also recommended the report back to Parliament on how authorised measures have been deployed including evidence of the extent to which the expected benefits and risks have been realised.

118 *Information Commissioner's Report to Parliament on the State of Surveillance*, (2010).

PART IV: CHARTING THE FUTURE

Part IV of the Report (CHARTING THE FUTURE) contains my proposals for change.

- **Chapter 13 (PRINCIPLES)** sets out the five principles on which my recommendations are founded:
    - Minimise no-go areas
    - Limited powers
    - Rights compliance
    - Clarity
    - Unified approach.
- **Chapter 14 (EXPLANATIONS)** is a commentary on the principal recommendations set out in Chapter 15, concerning in particular:
    - A clear and unified law
    - Definition of content and communications data
    - Data retention
    - The 2012 Communications Data Bill
    - Collection in bulk
    - Types of warrant
    - Extraterritoriality
    - Judicial authorisation
    - Use of intercepted material and data
    - Oversight: ISIC, the IPT and the ISC
    - Transparency
- **Chapter 15 (RECOMMENDATIONS)** sets out my 124 specific recommendations for reform.

13. PRINCIPLES

A question of trust[1]

13.1. I have described the public debate on investigatory powers as double-jointed, because it features arguments for more and fewer capabilities, more and fewer safeguards. The debate is also polarised: often characterised by exaggerated rhetoric and by a lack of trust between participants. In the words of one observer:

> "On one side there are civil liberties groups demanding increased privacy and transparency; on the other there are securocrats and law-enforcement spokesmen, under pressure to keep us safe and facing a bewildering array of security threats, insisting they need to monitor more of our online behaviour ... The debate is lurching between these nightmarish poles: we can choose a dystopia where our every move is secretly monitored, recorded and analysed, or a world where criminals are able to do what they like."[2]

Both sides are motivated by fear: not least, their common fear that technological change will throw into jeopardy what they hold to be most important.

13.2. The silent majority sits between those poles, in a state of some confusion. The technology is hard to grasp, and the law fragmented and opaque. Intelligence is said to have been harvested and shared in ways that neither Parliament nor public predicted, and that some have found disturbing and even unlawful. Yet this was brought to light not by the commissions, committees and courts of London, but by the unlawful activities of Edward Snowden. Informed discussion is hampered by the fact that both the benefits of the controversial techniques and the damage attributed to their disclosure are deemed too secret to be specified. Politics enters the picture, and for informed debate in the media are substituted the opposing caricatures of "*unprecedented threats to our security*" and "*snoopers' charter*".

13.3. If one thing is certain, it is that ***the road to a better system must be paved with trust***:

(a) Public consent to intrusive laws depends on people trusting the authorities, both to keep them safe and not to spy needlessly on them.[3]

(b) This in turn requires knowledge at least in outline of what powers are liable to be used,[4] and visible authorisation and oversight mechanisms in which the wider public, as well as those already initiated into the secret world, can have confidence.[5]

---

1 I chose the title of this Report before learning that it had been used for Onora O'Neill's BBC Reith Lectures of 2002. I have since read them, and gained some valuable insights.

2 J. Bartlett, *Orwell vs Terrorists*, 2015.

3 3.7, 10.14(g), 12.6 and 12.11 above.

4 7.27 and 12.16-12.17 above.

5 12.50, 12.82 and 12.83 above.

(c) Trust between strangers and within communities itself depends on assurance that the state will afford proper protection both to security and privacy.[6]

(d) Law enforcement and intelligence need clear boundaries, together with confidence that they will not be censured for acting within them and that their secrets will be protected.[7]

(e) Service providers (particularly the overseas providers whose cooperation is so necessary) crave the trust of their customers, and can earn it only by assuring them that their data will only be released in accordance with a visible legal framework and on ethical and independently controlled grounds.[8]

(f) Foreign governments (like the UK Government) need to know that data they choose to share is subject to proper safeguards.[9]

(g) People across the globe crave secure means of communication, and need to know that the UK can be trusted to comply in full with internationally recognised standards.[10]

13.4. Trust in powerful institutions depends not only on those institutions behaving themselves (though that is an essential prerequisite), but on there being mechanisms to verify that they have done so. Such mechanisms are particularly challenging to achieve in the national security field, where potential conflicts between state power and civil liberties are acute, suspicion rife and yet information tightly rationed.

13.5. 30 years ago, it might have been enough to appoint as independent reviewer (or Commissioner):

> "a person whose reputation would lend authority to his conclusions, because some of the information that led him to his conclusions would not be published".[11]

Respected independent regulators continue to play a vital and distinguished role. But in an age where trust depends on verification rather than reputation, trust by proxy is not enough. Hence the importance of clear law, fair procedures, rights compliance and transparency: not just fashionable buzz-words, but the necessary foundation for the trust between government and governed upon which the existence of coercive and intrusive powers depends in a modern democracy.

13.6. With the need to promote trust in mind, I have formulated my recommendations on the basis of the following principles: ***minimise no-go areas***, ***limited powers***, ***rights***

6 3.8(b) (security) and 2.11 (privacy) above.
7 9.91(a), 9.101 and 10.14 above.
8 11.4-11.9 above.
9 *R* (*Binyam Mohamed*) *v Secretary of State for Foreign Affairs* [2010] EWCA 65.
10 1.9 and 10.20 above.
11 Lord Elton, Hansard HL vol 449 cols 405-406 (8 March 1984). That remark from the Home Office Minister related to the independent reviewer of terrorism legislation, but similar considerations no doubt prompted the creation of the Interception Commissioner in the following year.

compliance, ***clarity*** and a ***unified approach***. Those principles are now explained in turn.

First principle: minimise no-go areas

13.7. A trusted system must be not only fair but effective. My first principle is that no-go areas for law enforcement should be minimised as far as possible, whether in the physical or the digital world.

13.8. It is often and correctly said that the first duty of the state is to ensure the safety of its citizens (or indeed all within its borders, irrespective of their nationality). Good order is a prerequisite not only for effective government in the public interest, but for the creation of a space in which individual and collective freedoms – including, among many others, the right to respect for private life – can be safely exercised. Only in a society whose institutions are protected from attack and in which there is an expectation that laws will be enforced is it possible for people to trust strangers, live without the fear of attack or intimidation, participate fully in the economy and society and develop to the full their own interests, personalities and quality of life.

13.9. The libertarian view that the State has no business snooping on the private affairs of the individual, and that some places or channels of communication should enjoy guaranteed immunity, has its attractions for some. But those attractions wane once it is recognised that there are individuals who will take advantage of any unpatrolled space to groom, abuse, blackmail, steal secrets from, threaten, defraud and plot destructive acts of terrorism against others. Any State that claims to protect its citizens must have the ability effectively to detect, disrupt and prosecute such behaviour. The central issue is how that ability can be combined with the expectation of privacy which law-abiding people have and deserve.

13.10. My first principle applies in the physical sphere. If the State is to discharge its primary duty of protecting its population, it needs the power to do the most sensitive things that can be imagined: bug a bedroom, search a safe, trick a person into a relationship, read a personal diary, eavesdrop on a conversation between lawyer and client or journalist and source. None of those things will be appropriate save in exceptional and occasional circumstances. Even then, they may well be completely impracticable to implement. But the issue is when it should be lawful to exercise such powers, not whether they should exist at all.

13.11. The same is true of the digital sphere. There may be all sorts of reasons – not least, secure encryption – why it is not physically possible to intercept a particular communication, or track a particular individual. But the power to do so needs to exist, even if it is only usable in cases where skill or trickery can provide a way around the obstacle. Were it to be otherwise, entire channels of communication could be reduced to lawless spaces in which freedom is enjoyed only by the strong, and evil of all kinds can flourish.[12]

[12] The metaphor of the "*ungoverned space*" is less apt. I do not suggest that law enforcement or intelligence should "*govern*" the internet: simply that they should have the ability to seek access to material and data when duly authorised to do so for a legitimate purpose.

13.12. This does not mean that state access to communications should be made easy. Few now contend for a master key to all communications held by the state, for a requirement to hold data locally in unencrypted form, or for a guaranteed facility to insert back doors into any telecommunications system. Such tools threaten the integrity of our communications and of the internet itself. Far preferable, on any view, is a law-based system in which encryption keys are handed over (by service providers or by the users themselves) only after properly authorised requests.

13.13. But in an imperfect world, in which many communications threatening to the UK are conducted over services whose providers do not or cannot comply with such requests, there is a compelling public interest in being able to penetrate any channel of communication, however partially or sporadically. Paedophiles should not be able to operate on the dark net with guaranteed impunity, and terrorists should not be able to render themselves undetectable simply by selecting an app on which their communications history will never be known even to the provider. Hence the argument for permitting ingenious or intrusive techniques (such as bulk data analysis or CNE) which may go some way towards enabling otherwise insuperable obstacles to be circumvented. Hence, also, the argument for requiring certain data to be retained so that they can be used in piecing together a crime after the event.

13.14. It has been argued that if western democracies refuse to accept no-go areas, the same will be true of undemocratic regimes that will use their access for sinister and brutal purposes. The prospect is a gloomy one. But the flaw in the argument is in the linkage that it asserts. Unpleasant regimes can (and do) use local control of the internet to suppress legitimate dialogue, self-expression and dissent: but neither their technical ability nor their inclination to do so are dependent on the practice of other countries. If the UK is to set an example to the world, it will not be by withdrawing from the dark spaces of the internet – a lead that no responsible government would choose to follow. It will be by demonstrating an ability to patrol those spaces in tightly defined circumstances, and with sufficient safeguards against abuse.

Second principle: limited powers

13.15. My second, balancing principle is that powers need to be limited in the interests of privacy.

13.16. What one might call over-governed spaces have existed from time to time in the physical world: commonly cited is the example of communist East Germany, where it has been estimated that there was at least one spy watching every 66 citizens.[13] But the practice of comprehensive physical surveillance is immensely difficult. There will always be suspicious groups which cannot be penetrated by a CHIS, buildings which cannot be safely bugged and potentially dangerous conversations which go undetected and unheard. Physical surveillance is also extremely costly, which tends to place its own limitations on what can be done. In no democracy has any of those techniques been employed against more than a tiny proportion of the population.

[13] J. Koehler, *Stasi – the untold story of the East German secret police*, 1999, chapter 1.

13.17. Things are very different in the digital world. Obligatory data retention requires service providers to retain and make available valuable communications data relating to, effectively, the whole population. Internationally, though GCHQ can access "*only a very small percentage*" of the 100,000 bearers that make up the structure of the internet and does not exercise "'*blanket' coverage of all communications*", the volume of communications travelling over those bearers is nevertheless "*extremely large*".[14] The availability of these techniques, and the relatively low marginal cost of using them, allow data to be harvested without any need for suspicion – an uncommon state of affairs where more labour-intensive powers are concerned.[15]

13.18. That is not to say that the interceptors and the collectors of communications data have it all their own way. Their resourcefulness is matched by that of cyber criminals and those who seek to threaten or undermine the State who, unlike them, are not constrained to behave ethically. The capabilities of the state are subject to technical or cost-based limits. But if the acceptable use of vast state powers is to be guaranteed, it cannot simply be by reference to the probity of its servants, the ingenuity of its enemies or current technical limitations on what it can do. Firm limits must also be written into law: not merely safeguards, but red lines that may not be crossed.

13.19. The point may be illustrated as follows. Some might find comfort in a world in which our every interaction and movement could be recorded, viewed in real-time and indefinitely retained for possible future use by the authorities. Crime-fighting, security, safety or public health justifications are never hard to find. So, to use a little imagination:

(a) A perpetual video feed from every room in every house (it being a serious criminal offence to obscure the lens), could reduce the incidence of domestic violence, even if the police undertook to view the record only on receipt of a complaint, and assist the detection of what remained.

(b) Blanket drone-based surveillance would ensure that criminals could not escape attention by holding their conversations outdoors.

(c) Electronic communications could be permitted only through the medium of licensed service providers, which as a licence condition would have to retain within the jurisdiction a complete plain-text version of every communication and make it available to the authorities on request.

(d) A constant feed of data from vehicles, domestic appliances and health-monitoring personal devices would enable the Government to identify suspicious (or life-threatening) patterns of behaviour, and take pre-emptive action to warn of risks and protect against them.

---

14 ISC Privacy and Security Report, paras 58-59.

15 There are no-suspicion powers in the physical world: see, e.g. the stop and search power in the Criminal Justice and Public Order Act 1994, s60, and the port stop power in the Terrorism Act 2000, Schedule 7, but even these are not exercised in a wholly random manner.

(e) The fitting of facial recognition software to every CCTV camera, and the insertion of a location-tracking chip under every individual's skin, would make successful kidnapping and abduction a thing of the past.

Some of those developments might even be possible without state compulsion: they would appeal to people concerned about their health or their families' safety.

13.20. Much of this is technically possible, or plausible. The impact of such powers on the innocent could be mitigated by the usual apparatus of safeguards, regulators and Codes of Practice. But a country constructed on such a basis would surely be intolerable to many of its inhabitants. A state that enjoyed all those powers would be truly totalitarian, even if the authorities had the best interests of its people at heart.

13.21. There would be practical risks: not least, maintaining the security of such vast quantities of data. But the crucial objection is that of principle. Such a society would have gone beyond Bentham's Panopticon[16] (whose inmates did not know they were being watched) into a world where constant surveillance was a certainty, and quiescence the inevitable result. There must surely come a point (though it comes at different places for different people) where the escalation of intrusive powers becomes too high a price to pay for a safer and more law-abiding environment.[17]

13.22. It may be objected that the result in combination of my first two principles is uncertain. They would deprive criminals of sanctuary, whilst imposing limitations (for the protection of the innocent) on the methods that can be used to catch them.

13.23. To that, I would answer as follows:

(a) ***It is how things are***: criminals and enforcers are locked in a digital arms race, where neither can be sure of having the upper hand.

(b) ***It is how things should be***. When no human institution is perfect, and when the great majority of those using private communications enhance blameless lives by doing so, it is right that there should be legal limits on when and how those communications may be intruded upon. That is so, even if those limits from time to time diminish the effectiveness of law enforcement and result in more bad things happening than would otherwise be the case.

13.24. Understanding the need for legal limits on state power is easier than knowing where those limits are to be placed. It is here that my third principle comes into play.

---

16 J. Bentham, *Panopticon*, 1787. The Panopticon was a design for a circular institutional building in which all could be observed by a central watchman, but none knew whether they were being observed or not. Promoted by Bentham as an enlightened model for a prison, the notoriety of the concept stems from the analysis of Michel Foucault in *Discipline and Punish*, 1975.

17 Or as Isabella Sankey of Liberty stated in evidence to the ISC: "*Some things might happen that could have been prevented if you took all of the most oppressive, restrictive and privacy-infringing measures. That is the price you pay to live in a free society*": ISC Privacy and Security Report, para 94.

Third principle: rights compliance

13.25. My third principle is that the state must respect internationally guaranteed rights and freedoms.

13.26. The UK's Parliament is sovereign. Almost uniquely in the world, it is untrammelled by the constraints of a written constitution; and even HRA 1998 places no constraints on its power to legislate as it pleases.[18] But the unbridled exercise of that sovereign power is liable to place the UK in breach of international legal obligations that it has freely chosen to observe. This means, in particular, that:

(a) Powers that intrude into the privacy of communications must be expressly provided for by ***accessible and foreseeable*** laws.

(b) Such powers may only be exercised when it is strictly ***necessary*** for the body in question to fulfil its legally prescribed mandate.

(c) Measures taken must be ***proportionate*** to the objective, meaning that the measure must be selected that least restricts human rights and that special care is taken to minimise the adverse impact of any measures on the rights of individuals, including in particular persons who are not suspected of any wrongdoing.

(d) There must be a clear and comprehensive system for the ***authorisation, monitoring and oversight*** of the use of any measure that restricts human rights.

(e) Individuals whose rights may have been infringed must be able to address complaints to an independent institution and seek an ***effective remedy***.[19]

Also in play are the UK's obligations to protect the ***freedom of expression*** (including by protecting journalistic sources), ***the freedom of assembly*** and the ***fair trial principle*** (including by respecting lawyer-client privilege). Even those rights are not absolute: under the ECHR, they may yield to sufficiently pressing considerations of national security and crime prevention.[20]

13.27. Whether described as human rights, civil liberties or fundamental freedoms, these rights assume their most prominent and enforceable form in the ECHR and the EU Charter. But the placing of privacy-related limits on legislative and executive power is more than a European phenomenon: it is a feature of all major international human rights instruments,[21] and of most constitutions. Indeed I was struck on my visits to the US and Canada by how often it was explained to me by Government or law

18 See 5.2 above.

19 Cf. M. Scheinin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight: UN General Assembly Human Rights Council, 17 May 2010, para 26.

20 See 5.21-5.22 above.

21 See, in particular, the ICCPR, drawn from the Universal Declaration of Human Rights (1948) and ratified by 167 states worldwide.

enforcement officials that a particular interference with privacy or personal data would be considered unconstitutional, or (in Canada) contrary to its ECHR-like Charter of Rights and Freedoms.

13.28. Central to most of these rights are the concepts of necessity and proportionality.[22] Because those concepts as developed by the courts are adaptable, nuanced and context-specific, they are well adapted to balancing the competing imperatives of privacy and security. But for the same reasons, they can appear flexible, and capable of subjective application. As a means of imposing strict limits on state power (my second principle, above) they are less certain, and more contestable, than hard-edged rules of a more absolute nature would be.

13.29. This highlights the vital importance of ensuring that where potentially intrusive powers are concerned, the necessity and proportionality tests are applied according to a thorough set of criteria, and in an independent spirit. However much credit one gives the state for its probity, one can understand those who have wondered whether a greater element of independence might occasionally have made a difference.[23] The paramount importance of independence is reflected in my recommendations regarding not only oversight (where effective though improvable independent mechanisms have already evolved in the UK) but authorisation.

13.30. To the principle that legally enforceable rights must be respected, I would add two riders:

(a) ***It is not always clear how far legal obligations extend***. Court challenges are currently pending or have very recently been resolved in relation to bulk collection, intelligence sharing, data retention, CNE, the protection of journalists' sources and legal professional privilege. It is not always possible to predict the ultimate outcome of such challenges, and nor is it the function of a report such as this to do so.

(b) ***Practices may be imperfect without being unlawful***. I have felt free to recommend change even when the law does not (or may not) require it. My recommendations aim to produce a modern, fair and workable law, not just one that may hope to survive future court scrutiny.

Fourth principle: clarity and transparency

13.31. The desire for legislative clarity is more than just tidy-mindedness. Obscure laws – and there are few more impenetrable than RIPA and its satellites – corrode democracy itself, because neither the public to whom they apply, nor even the legislators who debate and amend them, fully understand what they mean.[24] Thus:

(a) The scope of the RIPA Part I powers, and the precise nature of their interaction with other powers such as WTA 2006, is not apparent from their wording. Other

22 See 5.18-5.22 above.

23 See, e.g., Liberty's criticism of the alleged Optic Nerve programme. See Annex 7 to this Report and 12.68 above.

24 See the criticisms summarised at 12.20-12.23 above.

powers (TA 1984 s94; ISA 1994 ss 5 and 7) are so baldly stated as to tell the citizen little about how they are liable to be used.

(b) Obscurity was perpetuated by the paucity of litigation on RIPA Part I (itself a consequence of its covert operation) and by the Government's failure to indicate (at least until the Charles Farr Statement of 2014) how it interpreted the law.

(c) Recent amendments to DRIPA have been put through Parliament on either an urgent (DRIPA 2014) or expedited (CTSA 2015) basis, with the result that few parliamentarians were in a position to understand their full context and implications.

13.32. Confusing legal structures governing investigatory powers are not unique to the UK, as I discovered on my visit to the United States (where little-publicised executive orders add further complication). But countries which routinely intercept the communications and collect the data of persons outside their jurisdiction owe a special duty to ensure that at least the basic thrust of their laws can be understood by intelligent people across the world, without the aid of a highly specialised lawyer or a wet towel.

13.33. The fact that the subject-matter is technical is no excuse for obscurity. It should be possible to set out a series of limited powers, safeguards and review mechanisms with a high degree of clarity and (as RIPA itself demonstrated) without technical jargon: the place for the latter is in regularly updated Codes of Practice. The speed and unpredictability of technical change means that any statute is likely to need replacement (or at least significant updating) within 10 or 15 years. The use of technical language would tend to accelerate this outcome rather than delay it.

13.34. RIPA Part I has been patched up and mended a number of times, and could no doubt be kept on the road a little longer. It does not seem to me, however, that such a process would be sufficient to provide the clear and principled structure anticipated above. More is required if the law is to command public respect, at home and abroad. Accordingly, my recommendations are for a law that (while it would adopt much that is good in RIPA Parts I and IV) would replace them with a new statutory framework.

Fifth principle: a unified approach

13.35. The ISC Privacy and Security Report recommended that the Government should introduce a new Intelligence Services Bill, consolidating "*the intelligence and security related provisions*" of at least seven Acts of Parliament, including RIPA (Recommendation XX).

13.36. The Report did not recommend "*reforming RIPA*"[25] where other bodies were concerned (although, consistently with the scope of its own responsibilities, the ISC did not enquire into the use of RIPA by such bodies). The ISC envisaged that the police and other public authorities would not be covered by the new legislation, on the

[25] ISC Privacy and Security Report, p. 8 para xviii.

basis that (as it stated in a footnote) "*there should be a clear separation between intelligence and law enforcement functions*".[26]

13.37. The idea of consolidating duplicative powers over interception and communications data powers is a sound and (I have found) an uncontroversial one. My own recommendations are to the effect that equivalent powers to those in RIPA Part I should be brought within the same framework or at least made subject to equivalent conditions.[27]

13.38. More controversial is the idea that the law in this area should enshrine, for the first time, a clear separation between intelligence and law enforcement functions. It is true that such a separation is a feature of the laws of many other countries. Even in the UK, some statutory powers (notably those contained in ISA 1994 ss 5 and 7) are reserved to the security and intelligence agencies. The ISC's recommendation is therefore a perfectly logical one.

13.39. I do not however echo that recommendation, partly because I believe for the reasons stated above that RIPA Part I and associated powers require reform across the board, not just as they concern the security and intelligence agencies, and partly because it seems to me that to hive off the security and intelligence agencies in the manner suggested would be a retrograde step.

13.40. The seamless and cooperative working relationship between security and intelligence agencies and the police is a feature of the UK security landscape that is widely admired, but rarely successfully imitated, across the world. Part of the secret of that success is that police and agencies (in particular MI5) interoperate across significant parts of their work, a process that has accelerated since the London bombings of 2005. So, for example:

(a) MI5 works closely with counter-terrorism police not only in London but in other parts of the UK, for example in the four regional police Counter-Terrorism Units and four Counter-Terrorism Investigation Units across England and Wales and at major ports and airports.

(b) There is a similarly close relationship between MI5 and the NCA in the field of serious and organised crime.

(c) Police and MI5 each have their own investigative and surveillance teams, which use the same techniques, will often be interested in the same targets and may to some extent be used interchangeably.

13.41. Nor should the work of MI5 be distinguished from that of MI6 and GCHQ: it became evident to me during the course of the Review that they depend ever more on one another.

13.42. There are still investigatory powers that only the security and intelligence agencies deploy: notably, bulk data collection and CNE. I have not suggested that this should

---

26 *Ibid.*, fn 289.

27 Recommendations 6-7 below.

change. But as technology develops, bulk data analysis (notably by private companies) becomes a standard feature of everyday life and digital investigation techniques become more widespread, the trend may prove to be towards convergence rather than the reverse.

13.43. There is also the issue of oversight, and its effect on culture. Where investigatory powers are concerned, security and intelligence agencies, police and other public authorities are all subject to the unitary audit and inspection regime of IOCCO.[28] I welcome this. The degree of an intrusion into privacy is not affected by whether that intrusion is conducted by security and intelligence agencies or by police. Firm rules and strong oversight are as necessary in one case as they are in the other. To subject different public authorities to different sets of rules for essentially the same activities could give rise to a dilution in regulatory expertise, different standards of oversight (particularly if IOCCO were itself split down the middle), and ultimately – if a distinctive "*intelligence*" culture were to develop where the use of routine investigatory powers is concerned – different standards of conduct. It might even prompt a tendency to leave the exercise of intrusive powers to whichever body was perceived to be less strictly regulated. None of this would be welcome.

13.44. My fifth principle is, therefore, that there should be a single body of law, and a single system of oversight, for equivalent investigatory activities conducted by different public authorities.[29]

Recommendations – the objective

13.45. Applying the above principles in the light of the evidence submitted to the Review, a single new investigatory powers law will have to provide ***exhaustively***, ***clearly***, in a ***rights-compliant*** manner and with the maximum possible ***technological neutrality*** for:

(a) the ***types of measures*** permitted for the collection of data;

(b) the ***range of public authorities*** entitled to collect it;

(c) the ***objectives*** for which each type of collection measure can be used;

(d) the ***categories of person*** which may be subject to each type of collection measure;

(e) the ***threshold*** required to justify the use of each type of collection measure;

(f) the procedures for ***authorising*** each type of collection measure;

(g) the ***duration*** for which each type of collection measure can be applied;

---

28 It is not echoed in relation to RIPA part II, whose surveillance powers are audited by the ISCommr (in respect of the agencies) and the OSC (in respect of other public authorities). If my recommendations are followed, this distinction will cease to exist.

29 This is reflected in my Recommendations 1, 6 and 7.

(h) the types of data that may be held, and the criteria that apply to the ***use, retention, deletion and disclosure*** of those data;

(i) the ***parameters for sharing*** data and intelligence, including the conditions that must be met for intelligence to be shared, the entities with which intelligence may be shared and the safeguards that apply to exchanges of intelligence both domestically and internationally;

(j) an express prohibition on the use of foreign partners in any way that results in the ***circumvention*** of national legal standards and institutional controls;

(k) the maximum ***transparency*** that is compatible with effective operational use of the powers; and

(l) the procedures for ***overseeing and reviewing*** the use of collection measures and the analysis, use and sharing of data recovered pursuant to them.[30]

13.46. Where the interference with the right to respect for the privacy of communications is ***systematic*** rather than suspicion-based, "*[t]he sheer scale of the interference with privacy rights calls for a competing public policy justification of analogical magnitude*", including – as a minimum – "*a meaningful public account of the tangible benefits that accrue from its use*".[31] Enhanced procedures and safeguards may also be required when ***particularly sensitive rights*** are in issue, e.g. the right of journalists not to disclose their sources, and the right of a lawyer's client not to have his privileged legal communications disclosed.

13.47. Finally, it should never be forgotten that the state owes a primary duty to keep its people safe. Subject to all of the above, I recommend that public authorities should be provided with the ***tools needed effectively to combat the threats*** faced by the UK, its citizens and indeed those of other nations.[32]

13.48. In the remaining two Chapters, which should be read together, I indicate the thinking behind some of my principal recommendations, before listing the recommendations themselves.

---

30 Cf. M. Scheinin (UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism), Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight: UN General Assembly Human Rights Council, 17 May 2010, Recommendations 20-35.

31 Ben Emmerson QC (UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism), Report to the General Assembly of 23 September 2014, para 13.

32 Three examples of bulk data analysis delivering subjects to justice are at Annex 9 to this Report. Case studies 3, 5 and 6 helped other countries.

14. EXPLANATIONS

INTRODUCTION

14.1. The recommendations in Chapter 15 can be read on their own, but this Chapter provides some of my background thinking. It does not gloss every individual recommendation, but aims to explain, by going through the principal recommendations in numerical order:

(a) how they relate to earlier parts of this Report,

(b) why they were made, and

(c) why they take the form that they do.

14.2. The most detailed commentary in this Chapter relates to my recommendations on:

(a) ***Definitions of content and communications data*** (Recommendation 12, 14.11-14.12 below);

(b) ***Compulsory data retention*** (Recommendation 14, 14.14-14.22 below);

(c) ***2012 Communications Data Bill*** (Recommendations 15-18, 14.23-14.38 below);

(d) ***Bulk collection and bulk warrants*** (Recommendations 19 and 40-49, 14.39-14.45 and 14.72-14.77 below);

(e) ***Specific interception warrants*** (Recommendations 26-38, 14.60-14.63 and 14.68-14.70 below);

(f) ***Judicial authorisation of warrants*** (Recommendations 22, 30 and 47, 14.47-14.57 and 14.64-14.67 below);

(g) ***Collection of communications data*** (Recommendations 50-71, 14.78-14.86 below);

(h) ***Extraterritorial effect*** (Recommendations 24-25, 14.58-14.59 below);

(i) ***Use of intercepted material and data*** (Recommendations 72-81, 14.87-14.93 below);

(j) ***The Independent Surveillance and Intelligence Commission*** (Recommendations 82-112, 14.94-14.100 below); and

(k) ***The IPT*** (Recommendations 113-117, 14.101-14.108 below).

GENERAL (Recommendations 1-12)

14.3. Recommendations 1-9 give effect to my fourth principle (***clarity and transparency***) and my fifth principle (***unified approach***),[1] as well as to the legal requirement (illustrated by the judgment of 6 February in the Liberty IPT case) that powers will be lawful only if provided for in an ***accessible and foreseeable*** law.

14.4. Most of these recommendations have their origins in repeated submissions to the Review from civil society:[2] but they were willingly and ungrudgingly endorsed by almost everyone to whom I spoke, including within Government and the security and intelligence agencies.

14.5. Recommendation 4 encourages a radical departure from the convoluted structures and language of RIPA, and challenges the Office of Parliamentary Counsel to produce a ***clear, effective and readable*** text in accordance with their own aspirations and best practice. I explain at 1.9 above the special importance of ensuring that the new law can be understood by all those who debate it, apply it or are liable to be affected by it, in the UK or abroad.

14.6. Recommendations 6 and 7 seek to make the new law, so far as possible, both ***comprehensive*** and a ***one-stop shop*** for investigatory powers.[3]

14.7. Recommendation 9 deals with the ***avowal*** of intrusive capabilities, and underlines the ECHR Article 8 requirement that intrusive powers should be used only if provided for in a sufficiently accessible and foreseeable law. I emphasise that I am not aware of any sensitive capabilities which have not been avowed to the Secretary of State. Indeed I have been assured there are none.

14.8. Recommendation 10 (***restrictions on disclosure***) makes the point that if the use of controversial capabilities is to be properly debated and defended, including before the courts, the law must not place obstacles in the way of doing so other than those which are strictly required by the constraints of national security. It also picks up the need for clear rules on when intelligence can be shared, a point highlighted by the Police Ombudsman for Northern Ireland in a recent report.[4] There will be an additional reason for reviewing RIPA s19 if my Recommendation 99 is followed: see 14.103(b) below.

14.9. As to Recommendation 11 (***criminal offences***), there may be an argument for specific new criminal offences to be created (or higher penalties made available for existing offences), as suggested in the JCDCDB Report (paras 227 and 229), the ISC Privacy and Security Report (Recommendation T) and in the submission of Richard Greenhill to the Review. But it would be contrary to principle to render any breach of the Codes of Practice a criminal offence: this would enable the Secretary of State to create new criminal offences without proper parliamentary scrutiny, and would risk

1 13.31-13.44 above.
2 Chapter 12 above.
3 The non-RIPA powers referred to in these recommendations are introduced at 6.9-6.33 and 7.62-7.65 above.
4 In this respect I make no comment on the interpretation of RIPA or its predecessor statute IOCA 1985, but note that the Police Ombudsman referred to conflicting advice on the interpretation of IOCA and endorse his call for clarity.

destroying the benevolent culture of voluntarily confessing to error that successive IOCCs have remarked upon with approval.

14.10. Recommendation 12 (***definitions of content and communications data***) is of central significance for the construction of any new law.

14.11. As to the ***distinction between content and communications data***:

(a) The borderline is neither as clear nor as simple as when it could be explained in terms of the content of the letter versus the writing on the envelope.

- Communications data currently comprises some types of data (location data, and even some subscriber data) that can be quite revealing of personal habits and characteristics.[5]
- As is less often remarked, content (an undefined, residual category which includes anything not classified as communications data) comprises some material which is not particularly intrusive (e.g. a cookie, the date of a letter or the title of a file attached to an email: 10.28 above).
- There may be difficult cases at the margins, particularly in the esoteric technical sphere in which GCHQ operates.

(b) I do not recommend removing the distinction, despite the submissions referred to at 12.27-12.28 above. A difference in terms of intrusiveness between "*what is said or written*" on the one hand and "*the who, when, where and how of a communication*" on the other[6] is generally recognised, including in the practice of other States and in the case law of international courts.[7]

(c) But there is a case for (a) defining content in the new law[8] and (b) reviewing the borderline between content and communications data (in the new law or its Codes of Practice) so as to ensure that it reflects the reality of modern technology. CSPs pointed to web logs, cloud services and social media as areas of ambiguity: 11.36 above. Thought has undoubtedly been given to these matters within the security and intelligence agencies, but no proposal was ready to be put before me. Accordingly I recommend a review which should be as open and inclusive as possible.

---

5 The ISC coined the concept of "*Communications Data Plus*": Privacy and Security Report, March 2015, Recommendation W.

6 These helpful shorthand terms are used in the Acquisition and Disclosure of Communications Data Code of Practice, 2.12; cf. the 2013 Annual Report of the Interception of Communications Commissioner, April 2014, 4.2.

7 See, e.g., Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, CJEU 8 April 2014, para 39: knowledge of content affects the essence of privacy rights in a way that knowledge of other data does not.

8 As recommended in IOCCO's submission to the Review, December 2014, 3.2.6-3.2.7.

(d) In the meantime:

- I have assumed in my proposed scheme that a distinction between content and communications data will persist into the new law, and have reflected this in my proposals for authorisation.
- But in recognition of the fact that some communications data may be relatively intrusive, I have recommended that in some circumstances, including but not limited to privileged and confidential material, there should be judicial determination of an application to access communications data (Recommendations 68 and 70).

14.12. As to the ***subdivision of communications data*** into subscriber information, service use information and traffic data (6.6 above):

(a) That division is obscure,[9] old-fashioned,[10] relevant for only limited purposes[11] and not reliably based on the relative intrusiveness of the data sought.[12]

(b) The JCDCDB recommended almost three years ago that "*a new hierarchy of data types needs to be developed*" and that "*[t]here should be an urgent consultation with industry on changing the definitions and making them relevant to the year 2012*".[13] This has not taken place.

(c) I reiterate the JCDCDB's advice.[14] Any review should once again be as open and inclusive as possible, so as to dissipate the suspicion that attaches to any redefinition of terms in this area. It should also have in mind Recommendations 51 and 56 below.

CAPABILITIES (Recommendations 13-19)

14.13. Capabilities (leaving aside the recently-avowed CNE, which is currently the subject of litigation in the IPT: 7.64-7.65 above) are controversial in three main respects. These may be summarised as:

(a) ***Compulsory data retention***: whether CSPs should be obliged to retain certain types of communications data relating to all their customers for periods of up to

9 For example, one of the elements of the definition of s21(4)(b) "Service Use" information is that it "*contains none of the contents of a communication*"; yet the contents of a communication are nowhere defined in the Act.

10 See, e.g., "*subscriber information*": people "*subscribe*" to telephone services but not usually to apps used for internet communication.

11 6.7 above.

12 Subscriber information can be of a personal nature: 6.6(c) above.

13 JCDCDB Report, November 2012, paras 169 and 167.

14 It did seem to me that communications data might usefully and comprehensibly be reclassified by investigative purpose, taking as a starting point the categories originating in the Data Retention Directive and currently set out in the Schedule to the Data Retention Regulations 2014 (e.g. "*the internet service used*", "*data necessary to identify the date, time and duration of a communication*"). Everything else would be classified as content. But I have stopped short of making a recommendation in those terms: the issue is highly technical; the suggested approach was variously described by those I tried it out on as too broad and too narrow, and would require more thought; and in any event the issue should logically be considered only after the borderline between content and communications data has been decided upon.

12 months, as is currently the case under DRIPA 2014 s1 and CTSA 2015 s21 (and was previously the case under the EU Data Retention Directive).

(b) ***Communications Data Bill***: whether (as originally proposed in a Bill of 2012, dubbed by its opponents "*the snoopers' charter*") additional obligations should be placed upon CSPs, in particular as regards the retention of:

- records of subscribers' internet interactions (loosely known as web logs: see the Home Office definition of this term at 9.53 above); and
- the entire content of third-party communications that passed over the network of a UK CSP.

(c) ***Bulk collection***: whether GCHQ should be entitled to recover content and related communications data in bulk from cables carrying overseas traffic, as is currently permitted under RIPA s8(4), and to use it in specified ways for the purposes of protecting national security.

In framing my recommendations on capabilities, I seek to give effect to my first principle (***minimise no go areas***) as well as by the second (***limited powers***) and third (***rights compliance***).

Compulsory data retention

14.14. Recommendation 14 states that the data retention power now contained in DRIPA 2014 s1, as supplemented by the additional category of information whose retention is required by CTSA 2015 s21 (6.60-6.63 and 7.38 above) should remain in force after December 2016.

14.15. A comparative survey of compulsory data retention laws in Europe and the Five Eyes countries is at 8.55-8.59 above. Laws in Canada and Australia dating from 2014 and 2015 have made provision for compulsory data retention.

14.16. The utility of communications data to law enforcement across the board is explained at 7.43-7.51 and accompanying annexes. The experience of the police, NCA, CPS, Europol and European Commission in relation to the particular utility of retained data in criminal and missing persons investigations is at 7.49-7.51 and 9.43-9.47 above. The points made at 9.45 are of particular significance: older data may be the only way to catch the ringleader in a conspiracy, or to investigate a crime when months have elapsed between the incident and the identification of a suspect.

14.17. In order to test the utility of retained communications data, I decided to visit a country where data retention is not required, and to take evidence from law enforcement and from others. The obvious choice was Germany, where EU data protection rules apply as they do in the UK, but where the rules implementing the EU Data Retention Directive were struck down in March 2010 by the Federal Constitutional Court.

14.18. On a visit to Berlin in December 2014, I was able to question the Interior Ministry and internal security service (BfV) on the issue of data retention, together with the Federal Chancellery, the Justice Ministry, the Federal Data Protection Authority, Bitkom (an organisation representing CSPs) and academics who have reported on data retention.

My interlocutors spoke frankly, knowing that I would not attribute views to them or to their organisations in this report. But in summary, I took away the following:

(a) There is some non-compelled data retention: the criminal code allows data which have been retained for business purposes to be made available to the police. German CSPs currently keep data for up to 90 days in some cases, though generally much less. It was suggested to me by opponents of data retention that the utility of retained data falls off sharply after three months or so.[15]

(b) German law enforcement told me that a compulsory data retention requirement would be useful, particularly but not exclusively in relation to internet fraud and child pornography cases which they were increasingly unable to tackle. They continue to log examples of cases that they cannot pursue because retained data were not available.

(c) The enactment of a compulsory data retention law was however (since *Digital Rights Ireland*) off the political agenda.

(d) Public opinion (particularly in the west of the country) is strongly pro-privacy, partly because of 20th century historical experience and partly because there is little current exposure to terrorism, limited consciousness of cyber-crime and because people generally feel secure (or as one official put it to me, "*take security for granted*").

(e) Data preservation proposals (the so-called "*quick freeze*", under which preservation orders would be served only once a suspicion arises) were not being pursued. They are not considered an adequate alternative to data retention by German law enforcement, despite the apparent encouragement of the CJEU (5.68(c) above), and are considered technically problematic by some CSPs, which also had concerns about reimbursement.[16]

14.19. I put to my German interlocutors the very striking example given in the impact assessment that accompanied the DRIP Bill in 2014[17] of Operation Rescue, a major recent Europol investigation into international online child sexual exploitation. In the words of the impact assessment:

> "Of 371 suspects identified in the UK, 240 cases were investigated and 121 arrests or convictions were possible. In contrast of 377 suspects identified in Germany, which has no such data retention arrangements, only seven could be investigated and no arrests could be made."

Those familiar with the example did not deny the essential truth of this account, though a senior German academic commented that "*Most of these guys were only going to*

15 See however the UK police survey prepared for the JCDCDB, which found that 28% of all requests made by 62 UK law enforcement agencies over a two-week period in June 2012 were for data over three months old.

16 In the 2012 UK police survey referred to at 7.50(a) above, 28% of all data requests concerned people who were not suspects: 18% were victims.

17 Data Retention Legislation, IA No. HO0126, June 2014.

look: they would not actually have done anything" and that "*Missing one or two paedophiles is a reasonable price to pay for not having blanket intrusion*".

14.20. So while it is evident that German public attitudes (and thus the German political debate) are in a very different place from their UK equivalents, nothing I heard there causes me to question the strong law enforcement rationale for data retention that was pressed on me by UK police and others.

14.21. The CJEU in *Digital Rights Ireland* agreed that data retention could be "*a valuable tool for criminal investigations*" (5.67 above), and did not go so far as to suggest that compulsory data retention is unlawful. I commented at length on the *Digital Rights Ireland* judgment at 5.63-5.79 above. Whilst data retention was described by the CJEU as a "*particularly serious*" infringement of fundamental rights (5.78(b) above), I was referred to no concrete examples, whether in the UK or Germany, of harm to individuals caused by the retention of communications data in a country where proper safeguards regulate its use.

14.22. The meaning of *Digital Rights Ireland*, and its impact if any on DRIPA 2014, will no doubt be elucidated in the course of the proceedings begun by David Davis MP and Tom Watson MP: 5.75 above. The constraints of EU and of ECHR law of course have to be respected. But I am clear in my recommendation that data retention is a useful capability in fighting all kinds of crime, and that it should be retained in a manner that is consistent with those legal obligations.

Communications Data Bill

14.23. Recommendations 15-18 relate to the controversial matter of the draft Communications Data Bill, which was the subject of the JCDCDB Report of December 2012.

14.24. The centrepiece of the draft Bill was clause 1, an excessively broad power which would have allowed the Secretary of State, by order, to require CSPs to generate and collect all "*necessary*" communications data for the services and systems they provide, to retain it and to facilitate the efficient and effective obtaining of the data by public authorities.[18] This was said to be necessary in order to bridge a growing "*data gap*" which meant that even in 2012, "*approximately 25% of communications data required by investigators is unavailable*".[19]

14.25. The JCDCDB acknowledged the existence of a "*data gap*", but (noting the increased volume of communications data potentially available) resisted the Government's attempt to quantify it. It criticised the Home Office for assuming "*that a consultation paper published in April 2009 could justify publication of draft legislation three years later without further consultation with the public and with those most closely affected by its proposals*". The JCDCDB concluded:

18 JCDCDB Report, November 2012, para 61.
19 *Ibid.*, para 34.

> ".. that there is a case for legislation which will provide the law enforcement authorities with some further access to communications data, but that the current draft Bill is too sweeping and goes further than it need or should",

adding that:

> "[b]efore re-drafted legislation is introduced there should be a new round of consultation with technical experts, industry, law enforcement bodies, public authorities and civil liberties groups"

on the basis of a narrower, more clearly defined set of proposals.[20]

14.26. Those narrower proposals focussed on:

(a) subscriber data making it possible to ***resolve IP addresses*** (by indicating who is using a dynamic address at a particular time);

(b) records of user interaction with the internet, in the form of ***web log*** up to the first slash;

(c) the storage and disclosure by UK CSPs of ***third party data*** traversing their networks which relates to services from other providers; and

(d) the creation of a ***request filter***, described as "*a very complicated piece of technology*", to speed up complex inquiries and minimise collateral intrusion.[21]

14.27. The Home Office sought to take the recommendations of the JCDCDB into account and produced a pared-down draft Bill in early 2013, which I have been shown. However, the ensuing political paralysis on the subject of communications data has meant that save in relation to IP address resolution (which was addressed, in part, in CTSA 2015 s21), there has been no Government mandate to take matters forward over the past two years.

14.28. Though I asked Ministers in late 2014 for permission to show the draft Bill (or at least a summary of it) to CSPs with whom I discussed the issues, in particular at a lengthy meeting of the CDSG, that permission was not forthcoming. It became clear that in the absence of unified political will to progress the proposals, there has been little discussion of them with important stakeholders.

14.29. Meanwhile, the rest of the world has not stood still.

(a) Lord Blencathra, Chair of the JCDCDB, complained after publication of some of the Snowden Documents that Prism and the alleged Tempora programme[22] were "*highly, highly relevant*" to the JCDCDB's enquiry, but that the JCDCDB had not been "*even given any hint*" of their existence.[23]

---

20 *Ibid.*, November 2012, paras 36, 56, 281 and 284.

21 JCDCBC Report, November 2012, paras 121, 126.

22 Annex 7 to this Report, paras 3 and 5.

23 "Conservative peer Lord Blencathra hits out at online spying by GCHQ", Guardian website, 14 October 2013. Lord Blencathra was quoted as saying: "*Many of us are happy to have certain information collected by the state but, by God, we've a right to know the parameters under which they are operating*."

(b) The progress towards universal encryption has accelerated since the publication of the Snowden Documents, giving added force to the doubts expressed by the JCDCDB about the technical utility of the third party data proposal.[24]

(c) The *Digital Rights Ireland* decision of April 2014, with its sceptical approach to data retention even in the more limited form that was provided for in the Data Retention Directive, raises legal questions as to the more extensive powers mooted in the draft Bill.

(d) It was suggested to me at the CDSG meeting that I attended in early 2015 that the proposed request filter may have been overtaken by technological developments.

14.30. Though the position is sometimes opaque or hard to research, I am aware of no other Five Eyes or European country that provides for the compulsory retention either of web logs (9.55 above) or of third party data.[25] Such obligations were not considered politically conceivable by my interlocutors in Germany, Canada or the US. The 2015 Australian data retention law specifically exempts both web logs and third party data from the categories of data that must be retained by CSPs (9.55 and 9.64 above).

14.31. Against that legal, technical and comparative background, it seems to me that a high degree of caution is in order.

14.32. So far as ***web logs*** are concerned, the police and NCA asserted their operational utility for three purposes in particular (9.58-9.59 above):

(a) to help attribute communications to individual devices;

(b) to identify use of communications sites (allowing service providers to be approached for further detail); and

(c) to gather intelligence or evidence on web browsing activity, both on sites suggestive of criminality and more generally.

14.33. I have no doubt that retained records of user interaction with the internet (whether or not via web logs) would be useful for each of those purposes. But that is not enough on its own to justify the introduction of a new obligation on CSPs, particularly one which could be portrayed as potentially very intrusive on their customers' activities.[26] Though the submissions I received from law enforcement were emphatic about the value of such records, I was not presented with a detailed or unified case on:

---

24 JCDCBC Report, paras 91-101.

25 A recent comparative survey referred to (1) a Danish law of 2002 that provided for "*session logging*" (sampling the destination and source IP address of every 500th packet) until this requirement was removed in June 2014, reportedly because Danish police were unable to use the data, and (2) a recent Finnish Bill (HE 221/2013) which provided for retention of "*metadata produced from browsing of websites*", until this was removed after criticism from a parliamentary committee: Open Rights Group, "Data Retention in the EU following the CJEU ruling", April 2015.

26 The MPS suggested to me that the retained data would be useful for researching such matters as travel bookings and financial and property transactions: cf 9.59(b) above.

(a) the precise definition of the purposes for which such records should be accessible, and the relative importance of those purposes;

(b) the extent to which those purposes can in practice be achieved under existing powers (e.g. the inspection of a seized device), by less intrusive measures than that proposed[27] or by data preservation, i.e. an instruction to CSPs to retain the web logs or equivalent of a given user who was already of interest to law enforcement;

(c) the precise records that would need to be retained for the above purposes, and how those records should be defined;[28]

(d) the steps that would be needed to ensure the security of the data in the hands of the CSPs;

(e) the implications for privacy;[29] or

(f) the cost and feasibility of implementing the proposals.

14.34. That is perhaps not surprising, given that political will has been lacking to progress the issue. I am sympathetic to the operational case made to me by law enforcement, particularly in relation to the objectives at 14.32(a) and (b) above, and particularly if it is the case that a person's web browsing history cannot readily be deduced from the data that is retained.[30] The point was also made to me that even the sight of a person's web browsing history to the first slash (or equivalent), while unquestionably invasive of privacy, might be thought by some to be not necessarily more so than the sight of a person's phone log and/or location data.[31]

14.35. But privacy concerns are extremely strongly-felt in this area, as the international comparative picture makes clear, and it is clear to me (as it was to the JCDCDB, which came to no conclusion as to the acceptability of requiring web logs to be retained) that a good deal more preparatory work needs to be done. Before any detailed proposal is made, it will need to be carefully thought through and road-tested with law enforcement, legal advisers and CSPs. Outside technical experts, NGOs and the public should be consulted and given a full opportunity to comment. A strictly

---

27 For example, the purpose at 14.32(b) could in principle be achieved by requiring the retention of details relating only to communications sites: the JCDCDB Report of December 2012 recommended that the Home Office "*should examine whether it would be technically and operationally feasible, and cost effective, to require CSPs to keep web logs only on certain types of web services where those services enable communications between individuals*": para 88.

28 The NCA was reluctant to ask specifically for web logs to the first slash, making the point that destination IP addresses (which are numeric rather than textual, and analogous to a postcode rather than a house address) might be sufficient for some purposes (or for some CSPs). It also pointed out that the term web logs is inappropriate for non-web-based OTT apps that use IPs but not urls.

29 The Home Office emphasised to me that what they describe as a web log is far less informative (and thus immediately intrusive) than e.g. an Internet Explorer web browsing history, but acknowledged also that if there is an operational requirement it may, by using very sophisticated analysis tools, be possible to identify a specific page or group of pages visited. Independent experts broadly confirmed that position to me. The extent to which that "*stickiness*" is a guarantee of privacy, and will remain so as technology develops, is obviously vital to the proportionality of the proposed requirement.

30 Thus reducing the risk of intrusion if the data were to fall into the wrong hands.

31 Phone logs as well as browsing histories can tell when someone has contacted Alcoholics Anonymous or an AIDS helpline. But the development of a society which depends more on the internet than it ever did the telephone, together with specific factors such as the widespread use of pornography sites, may add further sensitivity to browsing histories.

evidence-based approach will be essential if this potentially useful initiative is to be progressed, especially bearing in mind the difficult legal climate summarised above.

14.36. The question of how access to such material should be authorised, and in particular when and how ISIC may need to be involved in addition to the normal mechanisms for public authorities to access communications data, will also need careful consideration in the event that a proposal is advanced.

14.37. As to compulsory ***retention of third party data*** – an extremely expensive part of the planned Communications Data Bill – I did not get the sense that this was judged to be the priority that it once was, even within law enforcement (9.64 above). The CSPs I spoke to about it were either actively hostile or felt remote from the debate since it was so long since they had been consulted. Some of the difficulties were identified in 2012 by the JCDCDB.[32] Three years on, the comments of the JCDCDB at 14.25 above remain apposite.

14.38. Accordingly, as stated in Recommendation 18, there should be no question of progressing this element of the old draft Bill until such time as a compelling operational case has been made, there has been full consultation with CSPs and the various legal and technical issues have been fully bottomed out. None of those conditions appears to me to be currently satisfied.

Collection in bulk

14.39. Recommendation 19 concerns the equally controversial subject of bulk data collection. The UK's current regime for the collection of bulk data has been exhaustively considered over the past year or so by:

(a) ***The IOCC***, in his reports of April 2014 and March 2015.[33] The limits on the power, and the safeguards on its operation, were meticulously set out and considered.

(b) ***The IPT***, in the Liberty IPT judgment of December 2014.[34]

(c) ***The ISC***, in its Privacy and Security Report of March 2015.[35]

Some of the most senior judicial and political figures in the country have therefore had the opportunity to analyse the regime and to comment upon it.

14.40. The IOCC and the IPT were not tasked with evaluating the statutory framework, but rather with assessing whether it was properly and lawfully operated. Nonetheless, each was exposed to the practical reality of that operation, including the full safeguards that operate to protect individual privacy. In that connection, it is significant that:

(a) The IOCC, having pointed out that there was a policy question as to whether the duly authorised interception agencies should continue to be enabled to

32 JCDCBC Report, paras 89-109.
33 IOCC Report of April 2014 at (6.5.27-6.5.58); IOCC Report of March 2015 at 6.23-6.40.
34 Liberty IPT Case, judgment of 5 December 2014, paras 61-152.
35 ISC Privacy and Security Report, chapters 4 and 5.

intercept external communications in order to assist their statutory functions, stated that he personally thought it "*obvious*" that, subject to sufficient safeguards, they should be.[36] In the same report he gave nine reasons, informed by his own detailed consideration, why "*the section 8(4) process does not have a significant risk of undue invasion of privacy*".[37]

(b) The IPT, though not tasked in that judgment with the consideration of proportionality, echoed and updated its own conclusion in 2004 that the s8(4) regime was "*in accordance with law*".[38]

14.41. The ISC concluded that "*GCHQ's bulk interception is a valuable capability that should remain available to them*" and that the legal safeguards protecting the communications of people within the UK were "*reassuring*": it made some specific suggestions for enhancing the safeguards.[39]

14.42. The law relating to bulk collection is dealt with in this Report at 6.45-6.59 above, its utility at 7.20-7.27 above (with accompanying Annex) and its importance for the security and intelligence agencies at 10.14(b) and 10.22-10.26 above. The opposition expressed in some civil society submissions is summarised at 12.35-12.38 above.

14.43. It is sometimes assumed that GCHQ employs automated data mining algorithms to detect target behaviour, as is often proposed in academic literature. That, it would say, is realistic for tasks such as financial fraud detection, but not for intelligence analysis. Much of its work involves analysis based on a fragment of information which forms the crucial lead, or seed, for further work. GCHQ's tradecraft lies in the application of lead-specific analysis to bring together potentially relevant data from diverse data stores in order to prove or disprove a theory or hypothesis. As illustrated by the case study on GCHQ's website,[40] significant analysis of data may be required before any actual name can be identified. This tradecraft requires very high volumes of queries to be run against communications data as results are dynamically tested, refined and further refined. GCHQ runs several thousand such communications data queries every day. One of the benefits of this targeted approach to data mining is that individuals who are innocent or peripheral to an investigation are never looked at, minimising the need for intrusion into their communications.

14.44. Contrasting reports on bulk collection have come out of the Council of Europe in 2015:

(a) A parliamentary committee reported in January that "*electronic mass surveillance is not even effective as a tool in the fight against terrorism and organised crime, in comparison with traditional targeted surveillance*", and calling upon Council of Europe member and observer states to cease bulk collection and analysis.[41] Its observations were founded, in part, on the

---

36 IOCC Report, April 2014, 6.5.56. It may be of interest to note that Sir Anthony May, who wrote those words, was one of the judges who ruled against the intelligence agencies in the well-known case of *R (Binyam Mohamed) v Secretary of State for Foreign Affairs* [2010] EWCA 65.

37 *Ibid.*, 6.5.43.

38 The ECtHR cases on bulk collection are discussed at 5.31-5.34 above.

39 See Recommendations F, P and generally at F-T.

40 "How does an analyst catch a terrorist?" (GCHQ website): 7.5 above.

41 PACE Committee on Legal Affairs and Human Rights, "Mass Surveillance", January 2015, para 126 and Resolution 17.1. The notion that bulk surveillance is not effective as a tool is contradicted by the

assessments of a study conducted under EU auspices, which has since gone on to conclude that "*[E]lectronic mass surveillance fails, and fails drastically. It produces at best medium-level usability scores which are overshadowed by a very high degree of ethical risk, coupled with levels of fundamental rights intrusion that on their own would make the surveillance legally impermissible under the EU Charter of Fundamental Rights and human rights treaties.*"[42]

(b) The European Commission for Democracy through Law (Venice Commission) reported in April 2015 in considerably more moderate (and on the basis of what I have seen, realistic) terms.[43]

- It accepted the utility of what it called "*strategic surveillance*", remarking on its importance for target development and locating it as "*one part of an overarching trend towards more proactive surveillance of the population*".[44]

- Having remarked that signals intelligence has historically been subject to relatively weak safeguards, partly because it grew out of military intelligence aimed at foreign communications,[45] it devoted most of its attention to the need for proper safeguards, regulation and oversight.

- It concluded that "*it is necessary to regulate the main elements in statute form and to provide for strong mechanisms of oversight*", observing that "*[t]he national legislature must be given a proper opportunity to understand the area and draw the necessary balances*".

14.45. Whether or not the s8(4) regime is proportionate for the purposes of ECHR Article 8 is an issue awaiting determination by the ECtHR. It is not my function to offer a legal assessment, particularly in a case that is under consideration by a senior court. But on the basis of what I have learned, there is no cause for me either to disagree with the factual conclusions expressed in recent months by the IOCC, the IPT or the ISC, or to recommend that bulk collection in its current form should cease. Indeed its utility, particularly in fighting terrorism in the years since the London bombings of 2005, has been made clear to me through the presentation of case studies and contemporaneous documents on which I have had the opportunity to interrogate analysts and other GCHQ staff. With such wide-ranging powers, it is however absolutely necessary that the right procedures and safeguards should be in place: I address this topic, with some suggestions for improvement, at Recommendations 40-49 and 72-80 below.

---

detailed examples I have been shown at GCHQ, six of which are reproduced in summary form at Annex 9 to this Report. One might wonder why, if it is not effective, it is practised at all.

42 SURVEILLE Deliverable D4.10, April 2015. Aspects of the SURVEILLE methodology seem debatable: some of the inputs are subjective in nature, and the potential of safeguards, regulation and oversight to reduce ethical risk seems not to have been taken into account.

43 European Commission for Democracy through Law, "Update of the 2007 Report on the democratic oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies", April 2015, CDL-AD(2015)006.

44 *Ibid.*, paras 51, 61, citing legal requirements on companies to retain and make available airline passenger name records, metadata and financial transactions data.

45 *Ibid.*, para 54.

INTERCEPTION AND ACQUISITION OF DATA (Recommendations 20-71)

14.46. Recommendation 20 sets out the types of warrant and authorisation that I have recommended should exist. These include the specific interception warrant, which would replace the current individual and thematic warrants, and the new bulk communications data warrant, which would enable bulk collection of communications data to take place without (as currently) needing to collect content at the same time. Recommendation 21 proposes that a similar scheme should be extended to the new powers referred to in Recommendation 6.

14.47. Recommendation 22 is to the effect that warrants should be judicially authorised. Following the submission to the Review of the Bingham Centre for the Rule of Law (12.23 and 12.52 above), I have suggested that the appropriate persons to perform this function would be senior serving or retired judges in their capacity as Judicial Commissioners.

14.48. The recommendation that Secretary of State authorisation be replaced by judicial authorisation is one of the more radical recommendations in this Report, since if adopted it would replace a practice of several centuries' standing.[46] But there is a precedent for it:[47] and notwithstanding the carefully reasoned contrary view of the ISC Privacy and Security Report,[48] I found it one of the easiest to arrive at.

14.49. My starting point was not any legal consideration, but rather the remarkable fact (at least to an outsider) that ***the Home Secretary routinely signs thousands of warrants per year***, most of them concerned with serious and organised crime and the remainder with national security (principally terrorism). The Home Secretary leads a huge department of state with responsibility for immigration and passports, drugs, policing, crime policy and counter-terrorism. Yet she has herself described warrantry as occupying more of her time than anything else (some of it on an urgent basis in the middle of the night). In 2014, the Home Secretary personally authorised 2,345 interception and property warrants and renewals: 7.33 above. Warrantry is no doubt approached by most Home Secretaries in a thoroughly conscientious manner,[49] and the Home Office WGD does an admirable job in supporting her. But it is open to question whether this function is the best use of the Secretary of State's valuable time.[50]

14.50. The second reason for recommending change is to ***improve public confidence*** in the system. I do not suggest that recent Secretaries of State have been complicit in

---

46 According to the report of the committee of Privy Councillors appointed to inquire into the interception of communications (1957, Cmnd 283), para 9, a proclamation of 1663 forbade the opening of letters save by warrant issued by the Secretary of State, but it appears to have formalised longstanding practice. See 2.20(a) above for the position in 1643.

47 In the report of the Joint Committee on Human Rights referred to at 12.50 above.

48 ISC Privacy and Security Report, March 2015, paras 194-203; Recommendations FF and GG.

49 As observed in the IOCC Report, April 2014, 3.40. But some, inevitably, will be more conscientious than others.

50 The Joint Committee on Human Rights made the same point in a report of 2007 (see 12.50 above), stating that in a 15-month period in 2006-07 the then Home Secretary had issued 2,243 warrants and modified 4,746 (though then as now, modifications were usually approved by a senior official within the WGD.) The Joint Committee said, mildly, that "*it must be difficult for the Home Secretary to give much scrutiny to each request*", and recommended that "*judicial authorisation replace ministerial authorisation other than in cases of genuine urgency*": paras 161-162.

the abuse of the warrantry system, so as to target people for political or otherwise improper reasons.[51] The professionalism of the WGD would make this difficult, at least in a blatant fashion. But neither the British public nor the global public can be counted on to take the probity of the Secretary of State on trust, a point pressed on me not only in the many civil society submissions on this point (12.50-12.53 above) but by a very senior police officer (9.91(a) above).

14.51. The third reason for recommending change relates to what the ISC has described as "*the single most important challenge that the Agencies face"*, which is no less a challenge for law enforcement: the difficulties in obtaining ***assistance from service providers based in the US***.[52] US companies which are used to a domestic system of judicial authorisation and not instinctively inclined to obey a UK warrant can find it difficult to understand why they should honour a warrant signed by the Secretary of State, as was impressed upon me in Silicon Valley (11.19 above) and as others have also observed.

14.52. The fourth reason for recommending change is that there is an ***established and well-functioning system for judicial approval*** by Commissioners of comparably intrusive measures, when applied for by the police: property interference, intrusive surveillance and long-term undercover police operations (which are adjudicated upon by the Commissioners even when they are sought on national security grounds).[53] I have spoken to four Surveillance Commissioners and been introduced to the tasks that they have to perform. Their experience (from a lifetime's court work) of police attitudes and methods renders them well qualified to judge whether an application is truly necessary and – if not – to send it back for reconsideration. The police also have the highest professional respect for the Commissioners, which is reinforced when the Commissioners go to speak to them about what they expect. Even if they had the necessary time to consider the detail, few Home Secretaries would have the same experience or expertise.

14.53. As to ***the legal position***, the ECHR considers that "*it is in principle desirable to entrust supervisory control to a judge*" but does not require judicial authorisation, at least where individual warrants are concerned.[54] It is possible however that a more independent authorisation mechanism may be required in the future, whether in relation to bulk warrants (where the need for robust safeguards is at its highest), or as a consequence of the CJEU's apparent insistence, in *Digital Rights Ireland*, on "*prior review carried out by a court or by an independent administrative authority*" even in respect of (less intrusive) access to retained communications data (5.68(f) and 5.79 above). Recommendation 22 would provide that independence.

14.54. Most intercepting authorities did not mind whether their warrants were issued by the Secretary of State or by a judge, so long as a quick turnaround could be achieved and urgency procedures were in place. The FCO was however insistent on ensuring that the proper function of the executive in relation to foreign affairs and national security

51 It was abuse of interception and other powers by the FBI and CIA in the US, and by the RCMP in Canada, which prompted the introduction of judicial authorisation in those jurisdictions after the reports of the Church Committee and McDonald Commission in the 1970s and early 1980s.

52 ISC Rigby Report, November 2014, para 460.

53 8.12, 8.15 and 8.19(c) above.

54 5.40-5.43 above; Liberty IPT Case, judgment of 5 December 2014, para 116(vi).

was retained (10.44 above). There was some resistance on the part of intercepting authorities to the idea of double authorisation, which was perceived as unnecessarily time-consuming.

14.55. The arguments classically advanced in favour of authorisation by Secretary of State are that the Secretary of State has ***democratic accountability***, that she is ***immediately available***,[55] that the business of warrantry keeps the Secretary of State ***well informed*** as to the threat, and (as the ISC argued at para 202 of its Privacy and Security Report) that the Secretary of State has the ability to take into account the ***wider context*** of the warrant application.

14.56. On those points:

(a) The Secretary State is in practice rarely if ever held politically accountable for the issue of warrants: contributing factors are RIPA s19, NCND and the fact that intercepted material is not admissible in court. The accountability that matters is in the IPT, and is the same regardless of who issued the warrant.

(b) There is no reason why a rota of Judicial Commissioners should not be as available – indeed more so – than a Secretary of State.[56]

(c) Civil servants are able to brief Ministers on the threat by means other than asking them to sign warrants.

(d) There are certainly cases, largely involving defence or foreign policy, in which the wider political context is crucial and the perspective of the Secretary of State a necessary one. That point is addressed in Recommendations 30 and 46, addressed at 14.64-14.65 below.

14.57. The ISC suggested that judges might approve more warrant applications than Ministers (Privacy and Security Report, para 203); but the Foreign Office made to me the opposite point: that judicial authorisation might "***disadvantage the UK***" because judges would be liable to refuse applications that Ministers accept. Were it the case that Ministers might be tempted to issue warrants in circumstances where it is illegal to do so, that would seem to me a strong argument in favour of judicial authorisation rather than against it.

Extraterritorial effect

14.58. The difficulties in securing cooperation from service providers overseas, particularly in the US, are described at 11.15-11.28 above and, in more detail, in the ISC's Rigby Report at paras 415-460. Recommendation 24 summarises my impressions of how a longer-term solution might look, after speaking to US service providers and to the US Government in December, but the decisive voice here will be that of Sir Nigel Sheinwald, the former British Ambassador to both the EU and the US, who was

55 As the Home Secretary said to the ISC: Privacy and Security Report, para 201.

56 The NCA complained of some difficulties in obtaining dates for signings by the Home Secretary: 9.91(b) above.

appointed by the Prime Minister in mid-2014 as Special Envoy on intelligence and law enforcement data sharing.

14.59. Recommendation 25 falls more directly within my remit. I understand those who argue that extraterritorial application sets a bad example to other countries, and who question whether it will ever or could ever be successfully enforced. It is certainly an unsatisfactory substitute for a multilateral arrangement under which partner countries would agree to honour each others' properly warranted requests, which must surely be the long-term goal. But some service providers find it easier to assist if there is a legal power purporting to require them to do so; and despite the fact that extraterritorial enforcement has not yet been tried, the presence on the statute book of DRIPA 2014 s4 has been of some assistance in securing vital cooperation from service providers. On that pragmatic basis I suggest that it should remain in force, at least for the time being.

Specific interception warrants

14.60. Recommendations 26-38 concern what I describe as "*specific interception warrants*", which like all other warrants must be issued by a Judicial Commissioner.

14.61. Currently, "*the very significant majority of 8(1) warrants relate to one individual*".[57] Limitation to a single person or premises would indeed appear to be required by the literal wording of RIPA s8(1). But the practice has developed of issuing "***thematic warrants***", which allow the same capability to be used against a defined group or network whose characteristics are such that the extent of the interference can reasonably be foreseen, and assessed as necessary and proportionate, in advance.[58]

14.62. The use of thematic warrants (which recall the practice in parts of Europe of issuing warrants in respect of a particular investigation without listing every individual target) has been a positive development – though caution has been needed, not least because there is no very clear backing for them on the face of RIPA s8(1). A single warrant application in respect of (for example) an organised crime group gives the intercepting authority the power to add or remove persons or premises from the warrant without recourse to the Secretary of State, which can be particularly useful in urgent or fast-moving cases. Thematic warrants can give both the issuing authority and the auditor a quicker and better grasp of the investigation than does a series of applications relating to different individuals. They can also help reduce the proliferation of documents of which the police complained to me (9.33 above).

14.63. My intention has been to encourage the use of thematic warrants (Recommendation 27), but within strict limits. The key issue here is the power of modification: I have recommended the addition of a new person or premises to the warrant should normally be for a Judicial Commissioner (rather than, as currently, for a senior official of a WGD), but that the function may be delegated by a Judicial Commissioner to a sufficiently senior DP if the circumstances so demand (Recommendation 34).

---

57 ISC Privacy and Security Report, March 2015, para 42.

58 *Ibid.*, paras 42-45; see also 7.15-7.16 and 10.38 above.

14.64. Recommendation 30, trailed at 14.56(d) above, is my suggested mechanism for reconciling judicial authorisation with the special expertise of the Secretary of State where the ***defence of the UK or its foreign policy*** are concerned. In short:

(a) Where a warrant (specific or bulk) is sought for a national security purpose relating to the defence of the UK or its foreign policy, I recommend that the Secretary of State should have the power to certify that the warrant is required in the interests of the defence and/or foreign policy of the UK. In the case of a bulk warrant, the Secretary of State should also have the power to certify that the warrant is required for the operation(s) and/or mission purposes identified on the warrant (Recommendation 46).

(b) The Judicial Commissioner should be able to depart from that certificate only on the basis of the principles applicable in judicial review:[59] an extremely high test in practice, given the proper reticence of the judiciary where matters of foreign policy are concerned.[60]

(c) Responsibility for verifying that the warrant satisfied the requirements of proportionality, and for authorising the warrant, would remain with the Judicial Commissioner.

14.65. The twin advantages of that arrangement are that it would preserve the proper role of the Secretary of State in relation to the assessment of the defence and foreign policy priorities of the country, whilst protecting the judges from being drawn into political or diplomatic judgements that are properly for the executive. The Judicial Commissioner would, of course, retain the ability to scrutinise such warrants for compliance, in respects falling outside the scope of the certificate, with the requirements set out in Recommendation 29 (specific interception warrants) and Recommendation 45 (bulk warrants). It seems to me proper that such scrutiny should remain with an independent judicial figure.

14.66. In such cases as in all others, the warrant-requesting authority would have a right to resubmit the application having remedied any defect identified by the Judicial Commissioner (Recommendation 33(a)), or indeed to ***appeal*** to the Chief Judicial Commissioner, a procedure modelled on that which is applied by the Office of Surveillance Commissioners (Recommendation 33(b)).

14.67. I do not consider it necessary to extend Recommendations 30 and 46 to national security warrants of a domestic nature. In particular:

(a) The same political and diplomatic considerations do not arise. Terrorism, which accounts for the bulk of national security warrants going through the Home Office, is criminal activity. The gathering of material on it for intelligence or law

---

59 There are parallels for this test in national security legislation: it is for example the basis on which the High Court must proceed when reviewing the determination of the Secretary of State's assessment of the need to impose a Terrorism Prevention and Investigation Measure (TPIM) under the TPIM Act 2011, s9(2).

60 It is difficult to imagine a warrant being refused on this basis, short of e.g. a complete lack of evidence that it might achieve the objective(s) sought.

enforcement purposes, including by means of interception, is not a political function.

(b) The capacity of judicial authorisation to allay public suspicions would be reduced if the Home Secretary were effectively given the power to decide whether a particular warrant was necessary in the interests of national security. National security being a term undefined in law, suspicious people (whether or not with good cause) will always criticise the exercise of that judgement by an elected politician whose views of what constitutes a national security threat may not coincide with those of an independent arbiter.

(c) The Surveillance Commissioners have become accustomed to considering the national security case for a long-term deployment of undercover police, and told me that they feel no uneasiness about doing so.

(d) There are considerable advantages in having a single warrant-granting authority rather than a dual arrangement. Under my scheme, the Home Office WGD could cease to exist, though it would be desirable for some of its resources and considerable expertise to be redeployed in ISIC.

14.68. Centrally important is the requirement that there be arrangements for the prompt consideration of ***urgent applications*** for specific interception warrants from any part of the UK and at any time (Recommendation 32).

14.69. Recommendation 37, to the effect that serious crime warrants should have the same ***6-month duration*** as national security warrants, responds to the recent comment of the IOCC that "*there remains a strong practical case for increasing the validity period for serious crime warrants to six months*",[61] with which I agree. Requesting authorities will have to apply effective procedures for the purpose of verifying that warrants proceed for cancellation once there is no further need them: an aspect that is already the subject of IOCCO inspections and that ISIC inspectors should also be astute to check.

14.70. Recommendation 38 removes a pointless distinction between RIPA Parts I and II as regards the date when warrant ***renewals*** take effect, allowing them to do so from with effect from the expiry of the original warrant as is currently the case under Part II. I am grateful to the ISCommr for drawing the discrepancy to my attention.

Combined warrants

14.71. Recommendation 39 relates to combined warrants, and is aimed at ensuring the necessary flexibility to perform interception, intrusive surveillance and property interference in the course of a single operation: see 10.36 above. It offers administrative convenience for any intercepting authority that might wish to make use of them, but does not dilute any protections, since the conditions for each type of warrant would still have to be satisfied.

61 IOCC Report, March 2015, 6.43.

Bulk warrants

14.72. Only the chiefs of the security and intelligence agencies should remain eligible to apply for bulk warrants (of which there are currently 20), and only with the approval of the Secretary of State (Recommendation 40). The issue of a bulk warrant should be for the ***Judicial Commissioner***, but with the same limitation as regards the national security case as was recommended in relation to specific interception warrants: Recommendations 46-47 and 14.64-14.66 above.

14.73. Recommendation 42b provides for ***communications data to be obtained in bulk*** without the accompanying content. It gives effect to the suggestion at 10.40(c) above, and could accommodate a range of different uses. To give an example of a circumstance where it might apply, bulk communications data is essential in identifying and illuminating particular types of activity on a network for the purposes of cyber-defence, where GCHQ is seeking to identify malicious activity on particular networks. This activity neither targets nor meaningfully intrudes into the communications of individuals. But more generally, such a warrant is self-evidently less intrusive than the current s8(4) warrant: hence the requirement (Recommendation 42) that a bulk content warrant should never be applied for, approved or authorised in circumstance where a bulk communications data warrant would suffice.

14.74. This additional power for the security and intelligence agencies to obtain communications data in bulk by warrant is not intended to replace the existing RIPA powers for law enforcement agencies to obtain large volumes of data directly from CSPs for cell-site analysis when it is necessary and proportionate to do so, for example when searching for or tracking the movements of a suspect, see 9.66.

14.75. Bulk warrants should remain available only in pursuit of the existing statutory purposes (Recommendation 43). But in lieu of the certificate provided for by RIPA s8(4)(b), which the ISC described as "*expressed in very general terms*" (6.49 above), the purposes for which material or data is sought should be spelled out by reference to ***specific operations or mission purposes***. I accept that those operations and/or mission purposes are likely to be numerous and (as in the example given in Recommendation 43: "*attack planning by ISIL in Iraq/Syria against the UK*") may themselves be fairly broad in nature. I believe though that this change will help focus minds on the specific reasons why bulk interception is said to be necessary, dispelling the notion that bulk warrants are "*untargeted*" and illustrating their kinship with the familiar concept, in many countries, of a thematic warrant that is issued in support of a particular operation.

14.76. The distinction between ***internal and external communications*** was widely attacked as arbitrary and misleading by civil society groups who made submissions to the review (12.25-12.26 above). I agree with them that the distinction is outdated in the context of internet communications and should be abandoned. Its value as a protection for persons inside the UK is limited in any event by the inescapable fact that a "*by-catch*" of internal communications is collected at the same time: for the purposes of the protection of persons within the UK, it is, rather, RIPA s16 which must

do the "*heavy lifting*" at the access stage: 6.53-6.54 above. (In that regard, I recommend a tightening of the s16 safeguard: 14.89 and Recommendation 79 below.)

14.77. Though it is at the access stage that the heavy lifting will still need to be done, I am unwilling to see a reduced level of ***protection at the collection stage for persons within the UK***, and so recommend that the internal/external safeguard on targeting not be removed, but rather made clearer so as to focus on the location of individuals rather than communications. Recommendation 44 proposes that bulk interception warrants should be required to be targeted at the recovery of intercepted material comprising the communications of persons believed to be outside the UK at the time of those communications. I have left open the question of whether any equivalent limitation is necessary or desirable in relation to bulk communications data warrants, which as noted at 14.73 above have the potential to be used for a variety of purposes which (at least in outline) should inform any parliamentary debate on the subject.

Authorisations

14.78. As to the acquisition of communications data otherwise than in bulk, my recommendations build on the existing scheme of DPs assisted by SPoCs, which is considered by all who have looked at it to provide robust and effective pre-authorisation scrutiny, as well as a measure of independence.[62] SPoCs should be provided for in statute (Recommendation 62).

14.79. Two matters that currently depend on the distinction between subscriber information, service use information and traffic data (which I have recommended should be reviewed: Recommendation 12) are the ***categories of communications data*** (if any) that should not be available to certain public authorities, and the ***rank or position required of a DP***. For that and for other reasons, each should be reviewed (Recommendations 51 and 56).

14.80. ***DPs within the security and intelligence agencies*** are not currently required to be independent from the investigation in which communications data is requested: they may indeed be the line manager of the analyst who seeks access to the data. The IOCC has recently reported that the selection procedure is undertaken "*carefully and conscientiously*", but also raised the question of whether might need to be some pre-authorisation or authentication process (or alternatively, enhanced audit).[63] The ISC, reporting on the same day, made a recommendation for independent authorisation which I have echoed in my own Recommendation 58.

14.81. Recommendation 58 would of course have to be implemented in a manner consistent with ECHR and EU law (including, should it be applicable in this context, the requirement of prior review referred to at 5.68(f) above). A manageable solution needs to be sought, based on an understanding of how bulk data is actually used (as to which, see 14.43 above), including by running very high volumes of requests before

62 The IOCC in his most recent report referred to the SPoC process as "*a stringent safeguard*", and after an exhaustive investigation did not find "*significant institutional overuse*" of communications data powers by police forces and law enforcement agencies: IOCC Report, March 2015, 7.46 and 7.94.

63 IOCC Report, March 2015, 6.38-6.39.

an individual has even been identified. There may be contexts, therefore, in which some kind of thematic approach will need to be considered.

14.82. Recommendation 66 would reverse the recently-imposed requirement on local authorities to seek ***judicial approval by a magistrate or sheriff*** for communications data requests. Whilst judicial approval at this level may sound like a safeguard, and was no doubt required for that reason, the reality appears to have been that it has added time, complexity and cost to the authorisation process without contributing additional rigour to it: 9.98-9.100 above. Indeed it is very likely that the introduction of this requirement has resulted in applications being made less often than they should: 9.100.

14.83. I considered recommending extra training for magistrates, or centralising the judicial mechanism in the court centres closest to NAFN's Tameside and Brighton offices:[64] an option that has been rejected in the past. But despite the fact that the requirement for authorisation by magistrate or sheriff was only recently introduced, I have no hesitation in advising its removal. The independent SPoCs of NAFN perform a good service (9.95 above) and – subject to careful audit by the Commissioners, and in conjunction with local authority DPs – should provide the requisite protection against the improper use of local authority powers to authorise the acquisition of communications data.

14.84. The "*ever-changing technical, jurisdictional and policy mish-mash*" that characterises the provision of communications data, particularly by overseas service providers (9.74 above), is notorious and makes it difficult for a SPoC to function effectively without a regular flow of work to keep skills and knowledge up to date. My suggested remedy, for which I encountered significant support, is to require all "***minor users***" of communications data (9.2-9.3 above), not just as at present the local authorities, to have the SPoC function performed for them centrally by NAFN: Recommendation 65.

14.85. ***Privileged or confidential material*** is dealt with in Recommendations 67-69:

(a) The DP of any public authority which seeks communications data for the purpose of determining matters that are privileged or confidential must either refuse the request or refer it to ISIC for determination by a Judicial Commissioner.

(b) When an application is not directed to such a purpose but relates to persons who handle privileged or confidential information (including doctors, lawyers, journalists, MPs or ministers of religion), special consideration and arrangements should be in place, and the authorisation should be flagged for the attention of ISIC.

14.86. The ***increased sensitivity of communications data***, and the ever-changing purposes for which it can be used, are acknowledged by Recommendations 70-71, which require requesting public authorities to refer novel or contentious requests to ISIC for a decision on authorisation. It is not intended that this should be a routine occurrence. As acknowledged in Recommendation 71, it will be essential to create a clear understanding of when it is appropriate. But in conjunction with ISIC's power to

64 Different solutions would have been needed for Scotland and Northern Ireland.

issue guidance for the benefit of requesting authorities[65] (Recommendation 95 above), this procedure presents an opportunity for judicial guidance to be offered (in the manner of guideline sentencing judgments, or the partly-published opinions of the FISA Court in the US and Federal Court in Canada) in relation to what is and is not appropriate in a fast-changing area.

USE OF INTERCEPTED MATERIAL AND DATA (Recommendations 72-81)

14.87. Recommendations 72-74 aim to ensure that:

(a) safeguards at least as strong as those currently in place should apply to the disclosure, dissemination, copying, storage and retention of intercepted material; and that

(b) equivalent safeguards should be provided in relation to communications data, backed by ISIC audits, extending to the processing of data for reasons going beyond their acquisition and to the use of data in conjunction with other datasets.

14.88. Recommendation 75, which supplements the more general references to the sharing of data in Recommendations 73(c) and 76-78, would ensure that so long as the security and intelligence agencies each operate the required safeguards, they may share intercepted material and communications data between themselves for the purposes of their respective statutory functions.

Use of material recovered under bulk warrants

14.89. Recommendation 79 would, if adopted, enhance the existing RIPA s16(3) safeguard on the use of intercepted material recovered under a bulk content warrant. It would do so by requiring a specific interception warrant, issued by a Judicial Commissioner, before content that relates to a communication involving a person believed to be in the UK could be read, looked at or listened to. This would strengthen the current requirement for a RIPA s16(3) modification, which the ISC said was "*unnecessarily complex and does not provide the same rigour as that provided by an 8(1) warrant*".[66] The likely increase in rigour will be all the greater if, as I have recommended, the successor to the s8(1) warrant is to be subject to authorisation by a Judicial Commissioner.

14.90. I do not however go so far as the ISC in recommending that the same enhanced protection should apply to UK nationals (though not the nationals of other states) when outside the UK.[67] The range of additional police powers and surveillance capabilities that exist within the UK is an objective reason for requiring the use of intercepted material recovered pursuant to a bulk warrant to be specifically warranted in the normal way: less intrusive means of obtaining the information may have been available. No such objective reason exists for favouring British nationals abroad, as

65 As in the *OSC Procedures and Guidance* booklet, December 2014, not publicly available, or (to take another possible model) the partially redacted Opinions that are issued by the FISA Court in the US and the Federal Court in Canada.

66 ISC Privacy and Security Report, March 2015, Recommendation Q.

67 *Ibid.*, Recommendation R.

was implicitly acknowledged when RIPA (progressively, by international standards) did not incorporate citizenship-based distinctions.

14.91. I have left open the question of what "*rigorous and rights-compliant procedures*" should apply for the purposes of authorising access to (1) content obtained under a bulk warrant and not relating to persons in the UK and (2) communications data obtained under a bulk warrant: Recommendation 80, and cf. Recommendation 76 above.

Intercept as evidence

14.92. As recorded at 9.16-9.18 above and in Recommendation 81, it is not the function of this Review to second-guess or to reinforce the eight reviews (some of them extremely detailed) which have, since 1993, failed to recommend that intercepted material be rendered admissible as evidence in court.

14.93. I do however recommend that consideration should be given to extending the already substantial list of exceptions from this rule to include the Parole Commissioners and Sentence Review Commissioners, both in Northern Ireland. There would be a possible benefit in terms of public safety: these bodies consider prisoner licence cases and have the ability to consider classified material in closed proceedings on the issue of whether persons convicted of serious offences remain a threat to the public. Allowing intercept to be admitted as evidence before them could enable the recall to prison of ex-prisoners on licence in respect of whom the evidence of continuing threat to the community comes from intercepted communications.

OVERSIGHT AND REVIEW (Recommendations 82-121)

Independent Surveillance and Intelligence Commission

14.94. Recommendations 82-112 concern the proposed new Independent Surveillance and Intelligence Commission (ISIC), which would be a well-resourced and outward-facing regulator both of all those involved in the exercise of surveillance powers and of the security and intelligence agencies more generally.

14.95. ISIC would merge the existing functions of its three predecessor Commissioners (including those only recently announced: bulk personal data and TA 1984 s94) and take on, in addition:

(a) the audit and inspection functions referred to in Recommendations 91-93;

(b) the warrant-issuing powers currently vested in the Secretary of State, to be exercised only by Judicial Commissioners who must hold or have held high judicial office, or Assistant Judicial Commissioners who have themselves held judicial office (Recommendations 84-88), and after hearing submissions from independent standing counsel where necessary (Recommendation 110(c));

(c) a new power to authorise communications data requests which are novel or contentious or which are made for the purpose of determining matters that are privileged or confidential (Recommendation 84(e)); and

(d) the ability to issue guidance as referred to in 14.86 above, and to participate in the preparation of Codes of Practice (Recommendation 84(f)).

14.96. A more general supervisory power over the activities of the security and intelligence agencies (Recommendation 97), and an enhanced reporting function (Recommendation 102) could also be considered for ISIC. Whether and when to do this would depend on the precise relationship between ISIC and the ISC, which is for others to decide (Recommendation 120) but which should in any event not involve an overlap of functions (Recommendations 97, 119).

14.97. ISIC would build on the considerable strengths of its predecessor Commissioners, which are founded on their strong judicial ethos, the trust that public authorities have in them and (in the case of IOCCO and the OSC) their professional and technically proficient inspectorates.[68] But its greater size and unified nature would give it a number of advantages over its predecessor Commissioners, notably:

(a) the ability to compare practice across the whole ***range of different public authorities***;[69]

(b) the ability to inspect the whole ***range of surveillance techniques***, thus aiding an appreciation of whether it was necessary and proportionate to use one technique rather than another;

(c) the ***gravitational force*** to attract excellent specialists (including technical specialists) whose opportunities are more limited in a smaller organisation; and

(d) the name recognition and ***public profile*** which has largely eluded its predecessor Commissioners, with the result that their work (and indeed their existence) have not been as widely known as they could have been (and should have been, granted the interest in surveillance matters following the publication of the Snowden Documents).

14.98. I have considered whether it would be difficult to combine the judicial authorisation function and the inspectorate in a single organisation, and concluded that it would not. A precedent already exists, in the form of the OSC whose six judicial Commissioners, three Assistant Commissioners and eight Inspectors all report, along with the secretariat, to the Chief Surveillance Commissioner (who from 1 July 2015 will be the former Lord Chief Justice, Lord Judge).[70] Whilst the judicial function is obviously a distinct one, there is considerable benefit in dialogue: the Judicial Commissioners could advise the inspectorate on matters to look out for on their inspections, and the inspectors could in turn suggest that a warrant be referred back to the Judicial Commissioners if they formed the impression that it was not being implemented as it should be, and that the Judicial Commissioners might wish to consider modifying or cancelling it.

---

68 The ISCommr has no inspectorate, and indeed had until recently the assistance of only one other person.

69 IOCCO already has that within its field of operation: the functions of the IntelISC and OSC are however divided between the intelligence agencies and the rest.

70 Figures taken from the organigram in the OSC Annual Report for 2013-14, September 2014, p 32.

14.99. ISIC should be willing and able to draw on ***specialist legal counsel***, including in relation to specific applications for warrants (Recommendation 110). and on ***expertise*** from the worlds of intelligence, computer science, technology, academia, law and the NGO sector (Recommendation 111). An ***international perspective*** is important. Though I did not in the end pursue the idea of an ISIC Ethics Committee to advise Judicial Commissioners on hard warrantry decisions,[71] still less the "*citizens' jury"* imaginatively proposed by Demos, it is vital that ISIC (including its Judicial Commissioners) should be exposed to a variety of informed opinion, including from intelligence professionals, technical experts, privacy advocates and the generation which has grown up online.

14.100. The ideal ***Chief Commissioner*** would be a former judge of the highest distinction who is willing to work the hours necessary to run a substantial organisation and open to public and media engagement, including (if e.g. an alleged scandal is brought to light) at short notice.[72] An illustrative model for how ISIC could thus be organised is at Annex 17 to this Report. Because the pool is small and there might be occasions on which no such candidate could be found, I have provided for the possibility of appointing as Chief Commissioner someone who is not a judge (Recommendation 104). In that event, a senior judge would act on a part-time basis as Chief Judicial Commissioner, not of course in a subordinate role in the ISIC hierarchy but leading the Judicial Commissioners on a self-standing basis as depicted in Annex 18 to this Report, whilst retaining the closest possible links with the Commission itself.

Investigatory Powers Tribunal

14.101. A brief history of the IPT is at 6.105-6.111 above, and some criticisms of it are summarised at 12.88-12.89.

14.102. As the IPT operates increasingly in the open (at least where legal issues are concerned) and produces more open judgments, it is likely increasingly to be perceived as a valuable and effective check on the exercise of intrusive powers.[73] Its merits include:

(a) the ability to hear cases without complainants needing to present even an arguable case that they are the subject of interference;

(b) the ability (not given to the Commissioners or ISC) to hear forceful adversarial argument and thus to clarify the issues;

(c) the ability to hold a public hearing on the assumption that facts asserted by the complainant are correct (thus circumventing at least some of the difficulties caused by NCND); and

(d) the RIPA s68(6) duty on public authorities to disclose information to IPT.

---

71 Though I am grateful for the useful research into Ethics Committees conducted for me by Grant Castle and Covington & Burling.

72 He or she could also be a serving judge, on the analogy of the chairmanship of the Law Commission, though there would be advantages in a Chair who was prepared to stay for longer than three years.

73 There has been an equivalent improvement in the public image of the US FISA Court, following the publication (if only in redacted form) of some of its Opinions.

In addition, the IPT has now moved its administrative base away from the Home Office to a location close to the Royal Courts of Justice: a welcome and necessary development.

14.103. My first two recommendations concern ***access to the IPT*** on the part of persons whose communications were wrongly intruded upon. I recommend, in accordance with suggestions submitted to me by IOCCO, that:

(a) the jurisdiction of the IPT should be expanded (or clarified) to cover circumstances where it is a CSP rather than a public authority which was at fault, for example, by intercepting the wrong communications address and/or disclosing the wrong communications data[74] (Recommendation 113); and that

(b) ISIC should be allowed to inform a subject of an error (subject to not prejudicing ongoing operations),[75] at least in cases where it considers it possible that the scale or nature of the error might entitle the subject of the error to compensation (Recommendation 99). A similar power might in principle be given to CSPs, but CSPs to which I spoke were more comfortable with a system whereby they would report errors to the Commissioners (as currently), who would take the necessary decision.

14.104. The second of those recommendations, though a departure from the current position, would still fall short of the general duty to notify (at least of interception) that exists in many countries and has been strongly encouraged (though not described as essential) by the European Court of Human Rights[76] and by a UN Special Rapporteur.[77] For as long as the relevant Commissioner's office does not inspect every intrusion, it will to some extent be arbitrary (or a matter of chance) whether an error is referred to the IPT or not. But improved procedures at IOCCO have made it more likely that serious errors will be uncovered by the sampling process. On any view, the existing threshold (wilful or reckless failure by a public body),[78] and its limitation to cases involving communications data or encryption keys, seem hard to understand.

14.105. My third recommendation is that there should be a ***right of appeal*** to an appropriate court[79] from rulings of the IPT, on points of law only (Recommendation 114). The IPT is unusual in being subject to no process of appeal, an incongruous state of affairs given that it is the only appropriate tribunal for certain categories of human rights appeals (RIPA s65(2)(3)), and that it can decide issues of great general importance involving vital issues of principle. The Court of Appeal is now accustomed to hearing

---

74 This was suggested by IOCCO's submission to the Review of December 2014, 3.1.4. IOCCO reported that in 2013, 20% of the interception errors and 12.5% of the communications data errors were caused by CSPs. A well-publicised example is the mistaken disclosure in March 2014 of more than 1000 numbers relating to News UK employees, inadvertently sent by Vodafone to the Metropolitan Police in the context of Operation Elveden.

75 There is no bar to this where communications data is concerned. It however currently falls foul of RIPA s19 where interception is concerned.

76 *Klass v Germany* (Application 5029/71, judgment of 6 September 1978) para 69; *AEIHR v Bulgaria* (2007) para 57; *Lüütsepp v Estonia* (Application 46069/13, pending).

77 UN Special Rapporteur on Free Expression A/HRC/23/40, 17 April 2013, para 82.

78 Communications Data Code of Practice, 8.3.

79 Appeal could lie to the Court of Appeal of England and Wales, the Inner House of the Court of Session or the Court of Appeal of Northern Ireland, as is the position for the Competition Appeal Tribunal.

appeals involving closed materials. It is desirable that human rights cases should be finally determined in the UK if possible; and if not, that the ECtHR should have the benefit of views reached after the benefit of argument in more than one court, and expressed at a very senior judicial level within the UK.

14.106. My fourth recommendation concerns ***declarations of incompatibility*** (Recommendation 115). HRA 1998 section 4(5) allows the higher courts to declare that a provision of primary legislation is incompatible with a Convention right, triggering the section 10 power to take remedial action. Consideration should be given to granting the IPT the same power, though this recommendation might be considered less important if my third recommendation is adopted, because there could then (depending on the basis of the decision) be the possibility of appeal to a court entitled to make a declaration of incompatibility.

14.107. Finally, it is important that the ***resources of the IPT*** should continue to be independent of those allocated to the Commissioners and to the ISC (Recommendation 116), and that it should be able to call on the assistance of ISIC as it has done the IOCC and ISCommr in recent years (Recommendation 117).

14.108. I decided not to make any recommendations concerning ***IPT procedures***, despite the calls to make available to it the procedures for dealing with closed material by the use of a security-cleared special advocate to represent the interests of the affected person. Such a procedure was first rolled out in the Special Immigration Appeals Commission ("SIAC") and more recently, by the JSA 2013, in the ordinary courts. But it can be argued that the nature of IPT cases reduces the need for an advocate to be able to take instructions on behalf of a claimant. There was also a strong belief in some quarters that counsel to the tribunal (whose role was described in the Liberty IPT Case)[80] is capable of having more influence in IPT closed procedures than would be attainable by a special advocate. So without dismissing the suggestion, I leave it for another forum or another day.

Intelligence and Security Committee

14.109. Recommendation 118 emphasises the importance (as did the recent Venice Commission report: 14.44(b) above) of having a parliamentary oversight committee in place. The future of the ISC is a matter for Parliament, and I am concerned only to ensure that its functions do not overlap with those of ISIC (Recommendations 119 and 120).

TRANSPARENCY (Recommendations 121-124)

14.110. As recognised in Recommendation 121, there are limits to how far transparency can go where operational matters are concerned.

14.111. My recommendations regarding transparency, which are important and self-explanatory, are at Recommendations 122-124.

80 Judgment of 5 December 2014, paras 8-10.

15. RECOMMENDATIONS

PRELIMINARY POINTS

- My task is not to adjudicate, but to design a better system. It should not be inferred from any suggestion for change that I consider the current arrangements to be unlawful.
- These recommendations aim to chart a course, but not to provide for every eventuality. They should be read accordingly.

GENERAL

1. RIPA Part I, DRIPA 2014 and Part 3 of CTSA 2015 should be replaced by a comprehensive new law, drafted from scratch, which:

   (a) affirms the privacy of communications;

   (b) prohibits interference with them by public authorities, save on terms specified; and

   (c) provides judicial, regulatory and parliamentary mechanisms for authorisation, audit and oversight of such interferences.

2. The new law should amend or replace RIPA Part IV. If Recommendation 82 below is adopted, changes will also be needed to Police Act 1997 Part III, RIPA Parts II and III and RIP(S)A.

3. The new law should be written so far as possible in non-technical language.

4. The new law should be structured and expressed so as to enable its essentials to be understood by intelligent readers across the world.

5. The new law should cover all essential features, leaving details of implementation and technical application to codes of practice to be laid before Parliament and to guidance which should be unpublished only to the extent necessary for reasons of national security.

6. The following should be brought into the new law and/or made subject to equivalent conditions to those recommended here:

   (a) the general power under TA 1984 s94, so far as it relates to matters covered by this Review (cf. ISC Report, Recommendation VV);

(b) equipment interference (or CNE) pursuant to ISA 1994 ss5 and 7, so far as it is conducted for the purpose of obtaining electronic communications (cf. ISC Report, Recommendations MM-PP);

(c) interception pursuant to WTA 2006 ss48-49 (cf. ISC Report, Recommendations XX-ZZ); and

(d) the acquisition and use of bulk personal data (cf. ISC Report, Recommendation X).

7. The new law should repeal or prohibit the use of any other powers providing for interference with communications. But for the avoidance of doubt, no recommendations are made in relation to the use of court orders to access stored communications (e.g. PACE s9) or the searching of devices lawfully seized, save that it is recommended that oversight should be extended to the former (Recommendation 92(d) below).

8. The new law should define as clearly as possible the powers and safeguards governing:

(a) the receipt of intercepted material and communications data from international partners; and

(b) the sharing of intercepted material and communications data with international partners;

(Recommendations 76-78 below).

9. Existing and future intrusive capabilities within the scope of this Review that are used or that it is proposed be used should be (cf. ISC Report, Recommendation BBB):

(a) promptly avowed to the Secretary of State and to ISIC;

(b) publicly avowed by the Secretary of State at the earliest opportunity consistent with the demands of national security; and, in any event,

(c) used only if provided for in statute and/or a Code of Practice in a manner that is sufficiently accessible and foreseeable to give an adequate indication of the circumstances in which, and the conditions on which, communications may be accessed by public authorities.

10. Within the constraints imposed by national security, the current restrictions and prohibitions relating to the disclosure of warrants and intercepted material (RIPA ss15 and 19, Official Secrets Act 1989 s4) should be clarified and reviewed (cf. ISC Report, Recommendation C) in order to ensure, in particular, that:

(a) there is no legal obstacle to explaining the uses (and utility) of warrants to Parliament, courts and public, and that

(b) as recommended by the Police Ombudsman for Northern Ireland in his report of 30 October 2014 on the Omagh bombing, there is "*absolute clarity as to how specific aspects of intelligence can be shared in order to assist in the investigation of crime*".

11. Breach of Codes of Practice should not automatically constitute a criminal offence: any new criminal offence or enhanced penalty (cf. JCDCDB Report paras 227 and 229; ISC Report, Recommendation T) should be specifically identified in the new law.

12. The definitions of content and of communications data, and any subdivisions, should be reviewed, with input from all interested parties including service providers, technical experts and NGOs, so as to ensure that they properly reflect both current and anticipated technological developments and the privacy interests attaching to different categories of material and data. Content and communications data should continue to be distinguished from one other, and their scope should be clearly delineated in law.

CAPABILITIES

Compulsory data retention

13. ATCSA 2001 Part 11 should be repealed, and the voluntary code of practice issued under it should be withdrawn.

14. The Home Secretary should be able by Notice (as under DRIPA 2014 s1 and CTSA 2015 s21) to require service providers to retain relevant communications data for periods of up to a year, if the Home Secretary considers that the requirement is necessary and proportionate for purposes laid down in Article 15(1) of the e-Privacy Directive.

Communications Data Bill

15. In relation to the subject matter of the 2012 Communications Data Bill, Government should initiate an early and intensive dialogue with law enforcement and CSPs in order to formulate an updated and coordinated position, informed by legal and technical advice, on the operational case for adding web logs (or the equivalent for non-web based OTT applications) to the data categories currently specified in the Schedule to the Data Retention Regulations 2014 for the purposes of:

(a) resolving shared IP addresses or other identifiers (in particular, to identify the user of a website);

(b) identifying when a person has communicated through a particular online service provider (so as to enable further enquiries to be pursued in relation to that provider); and/or

(c) allowing websites visited by a person to be identified (to investigate possible criminal activity).

Full consideration should be given to alternative means of achieving those purposes, including existing powers, and to the categories of data that should be required to be retained, which should be minimally intrusive. If a sufficiently compelling operational case has been made out, a rigorous assessment should then be conducted of the lawfulness, likely effectiveness, intrusiveness and cost of requiring such data to be retained. No detailed proposal should be put forward until that exercise has been performed.

16. The rules regarding retention of data by CSPs should comply (to the extent that it may be applicable) with EU law as contained e.g. in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* and with the ECHR, particularly as regards:

(a) limits on the data whose retention may be required;

(b) ensuring that retention periods are no longer than necessary;

(c) ensuring the protection and security of data and their destruction when the retention period ends; and

(d) the location in which data are stored.

17. To the extent that a requirement is placed on CSPs that may result in them retaining partial or complete web logs or equivalent, the circumstances in which access may be sought by public authorities and the conditions on which access should be granted should be the subject of guidance in a Code of Practice and/or from ISIC, and sufficient records should be kept to allow ISIC to verify through regular audit and inspection that requests have been properly authorised.

18. There should be no question of progressing proposals for the compulsory retention of third party data before such time as a compelling operational case may have been made, there has been full consultation with CSPs and the various legal and technical issues have been fully bottomed out. None of those conditions is currently satisfied.

Bulk collection

19. The capability of the security and intelligence agencies to collect and analyse intercepted material in bulk should be maintained, subject to rulings of the courts, but used only subject to the safeguards in Recommendations 40-49 and 72-80 below, and only in cases where it is necessary to achieve an objective that cannot be achieved by the new and less extensive power in Recommendation 42(b) below.

INTERCEPTION AND ACQUISITION OF DATA

Types of warrant and authorisation

20. In relation to interception and the acquisition of communications data, the following types of compulsory warrant and authorisation should be available:

(a) For the interception of communications in the course of transmission,

- an specific interception warrant
- a combined warrant
- a bulk interception warrant.

(b) For the acquisition of communications data in bulk, a bulk communications data warrant.

(c) For the acquisition of communications data otherwise than in bulk, an authorisation.

21. To the extent that Recommendation 6 above is adopted, the analogous activities there referred to should be subject to equivalent procedures.

22. Specific interception warrants, combined warrants, bulk interception warrants and bulk communications data warrants should be issued and renewed only on the authority of a Judicial Commissioner.

23. Authorisations for the acquisition of communications data otherwise than in bulk should be issued only on the authority of a DP authorised to do so by the authorising body.

Extraterritorial effect

24. It is not recommended that service providers wishing to offer services in the UK should be required to have a licence, or that they should be required to store data in the UK. But in order to address deficiencies in access to material from overseas service providers, the Government should:

(a) seek the cooperation of overseas service providers, including by explaining so far as possible the nature of the threat, how requests are authorised and overseen, and the steps that are taken to ensure that they are necessary and proportionate;

(b) seek the improvement and abbreviation of MLAT procedures, in particular with the US Department of Justice and the Irish authorities; and

(c) take a lead in developing and negotiating a new international framework for data-sharing among like-minded democratic nations.

25. Pending a satisfactory long-term solution to the problem, extraterritorial application should continue to be asserted in relation to warrants and authorisations (DRIPA 2014 s4), and consideration should be given to extraterritorial enforcement in appropriate cases.

Specific interception warrants

26. Only those persons currently specified in RIPA s6 should be entitled to apply for a specific interception warrant.

27. Specific interception warrants should be limited to a single person, premises or operation. Where a warrant relates to an operation, each person or premises to which the warrant is to apply, to the extent known at the time of the application, should be individually specified on a schedule to the warrant, together with the selectors (e.g. telephone numbers) applicable to that person or premises.

28. The only purposes for which a specific interception warrant can be issued should be, as under RIPA s5(3):

    (a) preventing or detecting serious crime (including by giving effect to a mutual legal assistance agreement), or

    (b) in the interests of national security (including safeguarding the economic well-being of the UK in a respect directly linked to the interests of national security).

29. Applications for interception warrants should contain the following information:

    (a) The background to the operation or investigation in the context of which the warrant is sought;

    (b) The person(s) or premises to which the application relates, to the extent known at the time of application, and how they feature in the operation;

    (c) A description of the communications to be intercepted, details of the service provider(s) and an assessment of the feasibility of the interception to the extent known at the time of application;

    (d) A description of the conduct to be authorised or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant;

    (e) An explanation of why that conduct is considered to be necessary for one or more of the permitted statutory purposes;

    (f) An explanation of why any likely intrusion into privacy is proportionate to what is sought to be achieved by that conduct, explaining why less intrusive alternatives have not been or would not be as effective;

    (g) Consideration of any collateral intrusion and why that intrusion is justified in the circumstances;

    (h) Whether the application is made for the purposes of determining matters that are privileged or confidential such as (for example) the identity or a witness or prospective witness being contacted by a lawyer or the identity of or a journalist's confidential source;

    (i) Whether the application relates to a person who is known to be a member of a profession that handles privileged or confidential information (including medical doctors, lawyers, journalists, Members of Parliament or ministers of religion), and if so what protections it is proposed will be applied;

(j) Where an application is urgent, the supporting justification;

(k) An assurance that all material intercepted will be kept for no longer than necessary in accordance with the applicable rules, and handled in accordance with the applicable procedures for minimisation, secure holding and destruction.

30. When a specific interception warrant is sought for the purpose specified in Recommendation 28(b) above (national security) and that purpose relates to the defence of the UK and/or the foreign policy of the Government, the Secretary of State should have the power to certify that the warrant is required in the interests of the defence and/or foreign policy of the UK. In such cases, the Judicial Commissioner in determining whether to issue the warrant (Recommendation 31 below) should be able to depart from that certificate only on the basis of the principles applicable in judicial review.

31. A specific interception warrant should be issued only if it is established to the satisfaction of a Judicial Commissioner that:

(a) the warrant is necessary for one or both of the permitted statutory purposes (Recommendation 28 above);

(b) the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct; and

(c) the assurances regarding the handling, retention, use and destruction of the intercepted material, including in relation to privileged or confidential material, are satisfactory.

32. Arrangements should be put in place for the prompt consideration of urgent applications for specific interception warrants from any part of the UK and at any time.

33. Should an application for a specific interception warrant be rejected, the Judicial Commissioner should give reasons for rejection. In the event of rejection, the applicant for a warrant should be able to:

(a) re-submit an amended application, addressing the defects or omissions identified by the Judicial Commissioner; or

(b) request a final ruling on the original application from the Chief Judicial Commissioner, by way of appeal from the original rejection.

The Chief Judicial Commissioner may consider any such appeal in conjunction with one or more other Judicial Commissioners.

34. It should normally be for a Judicial Commissioner to make major modifications to a specific interception warrant, e.g. the addition of a new person or premises to the schedule. So far as applicable, the information listed at Recommendation 29 above should be supplied and considered before such a modification is authorised. However, a Judicial Commissioner should have the power to authorise a DP meeting

the requirements set out in Recommendations 56 and 57 below to make major modifications to a specific interception warrant on the basis that such modifications are then notified promptly to the Judicial Commissioner. The circumstances in which this could be appropriate should be specified in a Code of Practice and might include, for example, (1) urgent or fast moving cases, and (2) cases in which the interference with privacy is always likely to be small, or to be consistent across possible targets.

35. Provision should be made for minor modifications (e.g. the addition of a new telephone number for an existing target) to be made, after consideration of the implications if any for privacy, collateral intrusion and proportionality, by a DP meeting the requirements set out in Recommendations 56 and 57 below.

36. A Judicial Commissioner should have the power to cancel a specific interception warrant at any time, if it appears to the Judicial Commissioner that one or more of the conditions for its issue are no longer satisfied.

37. Specific interception warrants should have a duration of six months. The Judicial Commissioner who issues the warrant should have a discretion to require that it be reviewed by a Judicial Commissioner at a specified time before its expiry.

38. Warrant renewals should take effect from the date of expiry of the warrant (as currently under RIPA Part I Chapter 2) rather than from the date of renewal (as currently under RIPA Part I Chapter 1).

Combined warrants

39. Combined warrants should be subject to the same rules as interception warrants, save that:

    (a) They may authorise, in the context of a given operation, more than one of (1) interception, (2) intrusive surveillance and (3) property interference.

    (b) They must explain why the conditions for each type of warrant are satisfied, and why it is necessary and proportionate for a combined warrant to be issued.

Bulk Warrants

40. Only the Director General of MI5, the Chief of MI6 and the Director of GCHQ, in each case with the approval of the Secretary of State, should be eligible to apply for bulk warrants.

41. The restrictions in Recommendation 27 should not apply to bulk warrants.

42. There should be two types of bulk warrant:

    (a) bulk interception warrants, which would allow content and related communications data to be obtained; and

    (b) bulk communications data warrants, which would allow only communications data to be obtained.

A bulk interception warrant should never be applied for, approved or authorised in circumstances where a bulk communications data warrant would suffice.

43. The purposes for which a bulk warrant is sought should be:

(a) limited to the permitted statutory purposes (Recommendation 28 above);

(b) in lieu of the certificate provided for by RIPA s8(4)(b)), limited to one or more specific operations or mission purposes (e.g. "*attack planning by ISIL in Iraq/Syria against the UK*").

44. Bulk interception warrants should, in addition, be required to be targeted at the recovery of intercepted material comprising the communications of persons believed to be outside the UK at the time of those communications. It should be determined (if Recommendation 42(b) is adopted) whether an analogous restriction is necessary or desirable in relation to bulk communications data warrants.

45. Applications for bulk warrants should contain the following information:

(a) The specific operation(s) or mission purpose(s) in respect of which they are sought;

(b) Description of the communications to be intercepted or acquired, details of the CSP(s) and an assessment of the feasibility of the interception or acquisition;

(c) Description of the conduct to be authorised, or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant;

(d) A statement specifying both the statutory purpose(s) and, as precisely as possible, the operations or mission purposes in relation to which material is sought;

(e) An explanation, backed by evidence, of why the interception or acquisition is considered to be necessary for one or more of the permitted statutory purposes and for the operations or mission purposes identified;

(f) An explanation of why any likely intrusion into privacy is proportionate to what is sought to be achieved by that conduct, explaining why less intrusive alternatives have not been or would not be as effective;

(g) Consideration of any collateral intrusion and why that intrusion is justified in the circumstances;

(h) Whether the application could result in acquisition of material or data that is privileged or confidential material, and if so what protections it is proposed will be applied;

(i) In the case of a bulk interception warrant, an explanation of why a bulk communications data warrant would not be an adequate alternative;

(j) In the case of a bulk communications data warrant, an explanation of why an authorisation would not be an adequate alternative;

(k) Where an application is urgent, supporting justification;

(l) Details of the use that it is proposed to make of the data that is recovered, including in relation to possible sharing and use in combination with other datasets;

(m) An assurance that all material recovered will be retained no longer than necessary, looked at, used or analysed only for certified purposes and in accordance with the applicable rules, and handled in accordance with the applicable procedures for minimisation, secure holding and destruction.

46. When approving a bulk warrant that is sought in whole or in part for the purpose referred to in Recommendation 28(b) above (national security), and when that purpose relates to the defence of the UK and/or the foreign policy of the Government, the Secretary of State should certify:

(a) that the warrant is required in the interests of the defence and/or foreign policy of the UK; and

(b) that it is required for the operation(s) and/or mission purpose(s) identified.

47. In such cases, the Judicial Commissioner in determining whether to issue the warrant (Recommendation 48 below) may depart from that certificate only on the basis of the principles applicable in judicial review.

48. A bulk warrant should be issued only if it is established to the satisfaction of a Judicial Commissioner that:

(a) its purpose and targets are limited by reference to the factors identified in Recommendations 43 and 44 above;

(b) it is necessary for one or more of the permitted statutory purposes;

(c) it is necessary for the mission purpose(s) and/or operation(s) identified;

(d) in the case of a bulk interception warrant, it is necessary for the warrant to apply to content as well as communications data;

(e) the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct; and that

(f) the assurances regarding the handling, retention, use and destruction of the intercepted material or acquired data, including in relation to privileged or confidential material, are satisfactory.

49. Recommendations 32-38 above should apply also to bulk warrants, save that any modification to a bulk warrant must be authorised by a Judicial Commissioner.

Authorisations

General

50. Public authorities with relevant criminal enforcement powers should in principle be able to acquire communications data. It should not be assumed that the public interest is served by reducing the number of bodies with such powers, unless there are bodies which have no use for them. There should be a mechanism for removing public authorities (or categories of public authorities) which no longer need the powers, and for adding those which need them.

51. The issue of which (if any) categories of communications data should be unavailable to certain public authorities should be reviewed, in the light of Recommendation 12 above and any revision of procedures for authorisation and review. (Some examples of the potential value to local authorities of what is currently known as traffic data are at Annex 16 to this report.)

52. The grounds on which communications data may be acquired should remain as set out in RIPA s22(2), subject to any limitation (relating, for example, to the need for crime to exceed a certain threshold of seriousness, which would not necessarily need to be set at the same level as in RIPA s81(2)(b)) that may be required by EU law or the ECHR.

53. Communications data should be acquired only after the grant by a DP of an authorisation. Details of the authorisation should be served on a CSP where it appears to the DP that the CSP is or may be in possession of, or capable of obtaining, any communications data. The distinction between an authorisation and a notice (RIPA s22) is unnecessary and should be abandoned.

54. The application for an authorisation should set out the matters specified in the Acquisition and Disclosure of Communications Data Code of Practice (March 2015) 3.5-3.6.

55. An authorisation should be granted only if the DP is satisfied, having taken the advice of the SPoC and considered all the matters specified in the application, that it is necessary and proportionate to do so.

Designated person

56. DPs should be persons of the requisite rank or position with the requesting public authority or another public authority. The Regulation of Investigatory Powers (Communications Data) Order 2010 should be revised after consultation in the light of:

(a) Recommendation 12 above;

(b) the comments of IOCCO (December 2014 submission to the Review, 3.3) on the appropriate rank of DPs and the need for consistency across public authorities and in relation to comparable methods of surveillance; and

(c) The new functions placed on DPs and summarised at Recommendations 59(b) and 60 below.

57. DPs should be adequately trained in human rights principles and legislation (including in relation to privileged or confidential material), and may grant authorisations only when and to the extent that it is necessary and proportionate to do so in the specific circumstances.

58. As recently stated in the ISC Report, Recommendation HH: "*there should always be a clear line of separation within the Agencies between investigative teams who request approval for a particular activity, and those within the Agency who authorise it*". DPs (including in the security and intelligence agencies) should be required by statute to be independent from operations and investigations when granting authorisations related to those operations and investigations, and this requirement should be implemented in a manner consistent with the ECHR and EU law.

59. The function of DPs should be:

(a) To authorise the acquisition of communications data (Recommendation 55 above);

(b) To make references to ISIC on applications for privileged/confidential material and, where appropriate, on novel/contentious applications (Recommendations 68 and 70 below).

60. In addition, DPs appointed by the nine bodies entitled to intercept communications data should be entitled to authorise minor modifications to specific interception warrants (Recommendation 35 above).

Single Point of Contact

61. No authorisation should be granted (save in exceptional circumstances specified in the new law) without the prior opinion of an accredited SPoC. The purpose of the SPoC should be:

(a) to ensure that only practical and lawful requirements for communications data are undertaken; and

(b) to facilitate the lawful acquisition of communications data, and effective co-operation between a public authority and CSPs.

62. The functions of the SPoC should be set out in statute along the lines of the March 2015 Code of Practice on the Acquisition and Disclosure of Communications Data, para 3.22.

63. SPoCs should not have to be located within the requesting authority. For example, there would be no obstacle to police SPoCs being organised on a regional or national level, as is NAFN.

64. In the case of local authorities, the SPoC function should continue to be compulsorily performed through a SPoC at NAFN.

65. In the case of the other "*minor users*", responsible between them for less than 1% of requests for communications data in 2014, the SPoC function should in future also be compulsorily performed by a SPoC at NAFN, which will need to be resourced for that purpose.

66. The requirement in RIPA 2000 ss23A-B of judicial approval by a magistrate or sheriff for local authority requests for communications data should be abandoned. Approvals should be granted, after consultation with NAFN, by a DP of appropriate seniority within the requesting public authority.

Privileged or confidential material

67. When the communications data sought relates to a person who is known to be a member of a profession that handles privileged or confidential information (including medical doctors, lawyers, journalists, Members of Parliament or ministers of religion), the new law should provide for the DP to ensure that (1) special consideration is given to the possible consequences for the exercise of rights and freedoms, (2) appropriate arrangements are in place for the use of the data, and (3) the application is flagged for the attention of ISIC inspectors.

68. If communications data is sought for the purposes of determining matters that are privileged or confidential such as (e.g.) (1) the identity or a witness or prospective witness being contacted by a lawyer or (2) the identity of or a journalist's confidential source, the DP should be obliged either to refuse the request or to refer the matter to ISIC for a Judicial Commissioner to decide whether to authorise the request.

69. A Code of Practice, and/or ISIC guidance, should specify (1) the rare circumstances in which it may be acceptable to seek communications data for such a purpose, and (2) the circumstances in which such requests should be referred to ISIC.

Novel or contentious cases

70. In recognition of the capacity of modern communications data to produce insights of a highly personal nature, where a novel or contentious request for communications data is made, the DP should refer the matter to ISIC for a Judicial Commissioner to decide whether to authorise the request.

71. A Code of Practice, and/or ISIC guidance, should specify the circumstances in which such requests should be referred to ISIC.

USE OF INTERCEPTED MATERIAL AND DATA

General safeguards

72. Safeguards at least equivalent to those in RIPA s15, as elaborated in Part 7 of the Interception of Communications draft Code of Practice, should ensure that the

domestic disclosure, dissemination, copying, storage and retention of intercepted material is limited to the minimum necessary for the authorised purposes.

73. Equivalent statutory safeguards should be provided in relation to communications data. In particular, the new law and a Code of Practice issued under it, with the involvement of the Information Commissioner as appropriate, should make provision for:

(a) why, how and where data are retained within public authorities;

(b) who may access them within the public authority;

(c) with whom the data may be shared, and under what conditions;

(d) the special rules needed as regards the treatment of data that appear to be privileged or confidential (see Recommendations 67-69 above), and data relating to a victim or a witness;

(e) the processing of data for reasons going beyond their acquisition;

(f) the use of data in conjunction with other datasets;

(g) the processes for determining which data should be destroyed or further retained; and

(h) compliance with DPA 1998.

74. These safeguards should be enforced and backed up by ISIC audits (as currently performed by IOCCO), examining:

(a) how the material and/or data were used or analysed;

(b) whether they were used for the stated or intended purpose;

(c) what actual interference or intrusion resulted, and whether it was proportionate to the aim set out in the original authorisation;

(d) whether the conduct became disproportionate to what was foreseen at the point of authorisation, and if so whether the operational team initiated the withdrawal of the authorisation;

(e) retention, storage and destruction arrangements; and

(f) whether any errors or breaches resulted from the interference or intrusion.

75. On the basis that MI5, MI6 and GCHQ each apply the safeguards referred to in Recommendations 72-73 above, they should be permitted to share intercepted material and communications data between them for the purposes of their respective functions.

76. Any receipt of intercepted material or communications data from third countries should be on the basis of clearly-defined safeguards, published save insofar as is necessary for the purposes of national security and monitored by ISIC, including a warrant governing any intercepted material that is sought (ISC Report, Recommendations QQ-TT).

77. Any transfer of intercepted material or communications data to third countries should be on the basis of clearly-defined safeguards, published save insofar as is necessary for the purposes of national security and monitored by ISIC.

78. The new law should make it clear that neither receipt nor transfer as referred to in Recommendations 76-77 above should ever be permitted or practised for the purpose of circumventing safeguards on the use of such material in the UK.

Use of material recovered under bulk warrants

79. Content that is acquired pursuant to a bulk interception warrant and that relates to a communication involving a person believed to be in the UK should be made available to be read, looked at or listened to only on the basis of a specific interception warrant issued by a Judicial Commissioner (Recommendations 26-38 above): cf. in part ISC Report, Recommendations Q and R.

80. The new law should in addition provide for appropriately rigorous and rights-compliant procedures for the purposes of authorising access to:

(a) content that is acquired pursuant to a bulk warrant and that does not relate to a communication involving a person believed to be in the UK; and

(b) (if Recommendation 42(b) is adopted), communications data that are obtained pursuant to a bulk warrant.

Intercept as evidence

81. The bar in RIPA s17 on using intercepted material as evidence in legal proceedings (recently endorsed after lengthy consideration in Cm 8989) did not form part of this Review. Consideration should however be given to adding to the list of exceptions in RIPA s18, without prejudice to any other possible additions, proceedings before (1) the Parole Commissioners for Northern Ireland and (2) the Sentence Review Commissioners in Northern Ireland.

OVERSIGHT AND REVIEW

Independent Surveillance and Intelligence Commission

82. The Interception of Communications Commissioner's Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (ISCommr) (the current Commissioners) should be replaced by a new Independent Surveillance and Intelligence Commission (ISIC).

83. It should be the duty of every relevant person to disclose or provide to ISIC all such documents and information as ISIC may require for carrying out its functions, as is the case for the current Commissioners under RIPAs s58 and 60 and the Police Act 1997 s107(5)(a).

Powers and functions

Warrants and authorisations

84. ISIC (through its Judicial Commissioners: see Recommendations 106-107 below) should be granted powers:

(a) to issue and renew warrants (Recommendation 22 above);

(b) to make major modifications to specific interception warrants and combined warrants (Recommendations 34 and 39 above);

(c) to make modifications to bulk warrants (Recommendation 49 above);

(d) to cancel warrants that it has issued (Recommendations 36, 39 and 49 above);

(e) to authorise applications for communications data referred to it by public authorities pursuant to Recommendations 68 (privileged and confidential material) and 70 (novel and contentious) above; and

(f) to issue guidance (cf. the OSC's Procedures and Guidance of December 2014) to public authorities in relation to issues arising in relation to applications for warrants and the grant of authorisations, which would supplement the new law and any codes of practice issued under it and which should be published where the constraints of national security permit.

85. The functions referred to in Recommendation 84 above should only be performed by Judicial Commissioners who hold or have held high judicial office (High Court or above), subject to the possibility of delegating certain functions to persons who hold or have held judicial office at least at the level of Circuit Judge. As currently with the OSC, the judicial authorisation function should be independent from and in no sense subordinate to the other functions of ISIC.

86. Judicial Commissioners should use their power where appropriate to request further clarification, information or documents from the requesting public authority, and/or to consult standing counsel on any point of legal difficulty. Public authorities should have a right of appeal to the Chief Judicial Commissioner (Recommendation 33(b) above).

87. ISIC (through its Judicial Commissioners) should also take over from the OSC its equivalent functions (in relation to public authorities other than the security and intelligence agencies) in relation to intrusive surveillance, property interference and undercover officers under RIPA Part II, RIP(S)A and the Police Act 1997.

88. ISIC should be resourced so as to enable it to provide a prompt, efficient and reliable warrantry service in all jurisdictions of the UK.

Audit and inspection

89. The existing audit and inspection functions of the current Commissioners should be transferred to the ISIC, including:

(a) all those set out in RIPA Parts I-III, RIP(S)A and the Police Act 1997, to the extent that they are consistent with the arrangements in the new law;

(b) the audit of the use by security and intelligence agencies of their holdings of bulk personal datasets (cf. ISC Report, Recommendations X and Y); and

(c) the recently granted power to oversee the operation of directions under TA 1984 s94 (IOCCO Report, March 2015, section 10), to the extent that such power may survive the introduction of the new law.

90. ISIC should have the power to review compliance with the terms of any warrant, authorisation or guidance that may have been issued by the Judicial Commissioners. Where error is found, an Inspector should be able to recommend that the warrant in question be reviewed by a Judicial Commissioner with a view to its possible modification or cancellation.

91. In addition, ISIC should have the power to inspect:

(a) The exercise by DPs of all the functions summarised in Recommendations 59 and 60 above;

(b) The treatment by public authorities of privileged and confidential material;

(c) The retention, storage, processing and destruction of all communications data acquired by public authorities (not just, as currently for IOCCO, communications data only when it is related to intercepted material);

(d) The use of such data, including in combination with other datasets (cf. ISC Report, Recommendation Y);

(e) The use by public authorities of open-source intelligence (OSINT);

(f) The sharing of intercepted material and communications data within the UK Government;

(g) The receipt of intercepted material and communications data from, and the transfer of such material and data to, foreign governments (Recommendations 76-78 above).

92. Additional gaps in the arrangements relating to IOCCO's current activities (explained in IOCCO's submission of December 2014 to this Review) should be filled when ISIC is constituted. In particular:

(a) Express provision should be made for error reporting, and for a procedure for arriving at and keeping under review the definition of an error where interception is concerned.

(b) There should be a statutory requirement for ISIC to review the giving of notices by the Secretary of State (currently under DRIPA 2014 s1) requiring the retention of specific communications data by a CSP.

(c) ISIC should have the power to report on refusals by service providers (including overseas service providers, given the extraterritorial effect of the law) to intercept communications or disclose communications data when a lawful request is made of them.

(d) There should be statutory provision for oversight of the operation of powers for interception and/or obtaining communications data other than in the new law, to the extent that such powers survive, including the power to access stored data by order of the court under PACE s9.

93. Though strictly outside the scope of this Review, it would also be appropriate to review the existing powers of the OSC and of the ISCommr so as to identify any other gaps that should be filled when constituting the ISIC.

94. ISIC (like IOCCO before it) should have the capacity to inspect the work of analysts, investigators, SPoCs and DPs on live cases as well as on cases that are closed.

95. ISIC should have the power to report on, to issue guidance on and to participate in the preparation of Codes of Practice for any activity which it has the power to inspect.

Intelligence oversight functions

96. ISIC should inherit the intelligence oversight functions of the ISCommr, including:

(a) oversight of the Consolidated Guidance to Intelligence Officers and Service Personnel; and

(b) keeping under review the activities of the security and intelligence agencies or others engaging in intelligence activity, as directed by the Prime Minister under RIPA s59A.

97. Consideration could be given to granting ISIC a more general supervisory power over the activities of the security and intelligence agencies, but subject to Recommendations 118 and 119 (no duplication of functions and resources).

Powers relating to the IPT

98. ISIC should be subject to the same obligation as the current Commissioners (RIPA s68(2)) to provide assistance to the IPT, and should be kept informed of proceedings relevant to its functions (as by RIPA s68(3)).

99. ISIC should further be given the power, on its own initiative or at the suggestion of a public authority or CSP, and subject to a duty not to disclose anything that would be damaging to national security or prejudice ongoing operations, to:

(a) inform a subject of an error on the part of a public authority or CSP; and

(b) inform the subject of his right to lodge an application to the IPT;

in any case in which in the opinion of ISIC it is possible that the scale or nature of the error might entitle the subject of the error to compensation.

Analogous activities

100. To the extent that Recommendation 6 is adopted, the powers and functions set out in Recommendations 84-99 above should apply in an equivalent manner to the activities there referred to.

Reporting

101. There should be a report at least once in every year dealing with all aspects of the work of ISIC, and supplemented as may be feasible by more regular statistical releases.

102. As an expert, apolitical body with a strong judicial ethos, ISIC should also have the power to carry out inquiries and produce reports into matters falling within its remit, at the request of the Prime Minister or on its own initiative.

103. The Prime Minister should have the power to redact ISIC's annual report on narrowly specified grounds (cf. RIPA s58(7)). The Prime Minister should be obliged to lay ISIC's annual report before Parliament within a certain number of days (or sitting days) of receipt.

Organisation and working methods

Chief Commissioner

104. The Chief Commissioner should be a person of unquestioned professional distinction and independence, committed not only to leading the work of ISIC but to accounting publicly and to Parliament for that work, and to building public awareness of ISIC and its role. The Chief Judicial Commissioner should be eligible to serve also as Chief Commissioner, but need not necessarily do so: some possibilities are illustrated in the diagrams at Annexes 17 and 18 to this Report.

105. The Chief Commissioner should be appointed by the Prime Minister. Consideration should be given to allowing the ISC a voice in the appointment or confirmation of the Chief Commissioner.

Judicial Commissioners

106. Judges entitled to authorise warrants should be known as Judicial Commissioners (or Assistant Judicial Commissioners) so as to emphasise their distinct and independent status. There should be regular dialogue and sharing of experience between the Judicial Commissioners and the inspectorate.

107. Judicial Commissioners could be full-time or (as currently in the OSC) part-time judges on duty according to a rota. They should be capable of providing prompt and efficient service for applications from all parts of the UK. It will be necessary to provide 24-hour cover (as currently provided by the Secretary of State) for cases where urgent applications for warrants and authorisations arise out of hours.

Inspectorate

108. An inspectorate should be provided for the audit and inspection functions entrusted to ISIC.

109. ISIC should have staff with the necessary expertise (including technical expertise) and resources in relation to:

(a) each power whose operation it audits or inspects (including interception and encryption, communications data, directed and intrusive surveillance, property interference and CHIS/undercover operations); and

(b) each function relating to intercepted material and data (including acquisition, use, storage, retention, dissemination, sharing and destruction).

Legal

110. ISIC should have an in-house legal presence and one or more security-cleared standing counsel, appointed on a part-time basis from the independent practising Bar, whose function would be, on request:

(a) to give advice on recent developments in the law;

(b) to advise ISIC on possible legal vulnerabilities in the arrangements whose operation it reviews;

(c) to advise (at the request of the Judicial Commissioners) in relation to applications for warrants or requests for authorisations on proposed communications data authorisations;

(d) to assist with the legal aspects of formulating guidance and contributing to Codes of Practice; and

(e) by these means to help ISIC ensure that the activities it authorises, audits or reviews are lawful, and that the public authorities it oversees have due warning of legal difficulties.

General

111. Within the necessary constraints of security:

(a) ISIC should be public-facing, transparent and open to diverse ideas (including from all sectors of the community in all parts of the UK, from other countries, from international institutions and from young people who have grown up online).

(b) It should be willing to draw on expertise from the worlds of intelligence, computer science, technology, academia, law and the NGO sector, and should engage with and support compliance officers and compliance mechanisms within public authorities, DPs and SPoCs.

(c) As much as possible of its output (including, within the constraints of national security, any guidance that it may issue) should be published on a user-friendly website.

(d) Commissioners and staff should attend and participate in conferences, invite dialogue, assist the conduct of research and be alert to the adoption and dissemination of international best practice.

(e) ISIC should make itself accessible to traditional media, and have an active social media presence.

112. ISIC should be sufficiently resourced to enable it to perform functions which are more extensive than those performed by the almost 40 full-time and part-time current Commissioners and staff.

Investigatory Powers Tribunal

Access to the IPT

113. The jurisdiction of the IPT should be expanded (or clarified) to cover circumstances where it is a CSP rather than a public authority which was at fault (for example, by intercepting the wrong communications address and/or disclosing the wrong communications data).

114. There should be a right of appeal to an appropriate court from rulings of the IPT, on points of law only, permission being required in the normal way from either the IPT or the appellate court (cf. ISC Report, Recommendation LL).

115. The IPT (which is chaired by a High Court Judge or Lord Justice of Appeal) should be given the same power as the High Court to make a declaration of incompatibility under HRA 1998 s4, particularly (but not exclusively) should Recommendation 114 not be adopted.

116. The IPT should have the resources it needs to operate in a practical and expeditious manner. Those resources should be independent of those allocated to ISIC and the ISC, whose conduct may from time to time be in issue before the IPT.

117. The IPT should where appropriate require ISIC to provide it with assistance, particularly of an investigative nature, as it has several times required the existing Commissioners to do pursuant to RIPA s68(2).

Intelligence and Security Committee

118. There should continue to be a committee of parliamentarians with oversight of the work of the security and intelligence agencies and trusted by them with classified information, not only because parliamentary oversight is desirable in principle but because of the knowledge and understanding that its members bring to parliamentary debates with national security implications, e.g. in relation to terrorism legislation and proscription orders.

119. The functions of ISIC and the ISC should not overlap. In particular, there should be no duplication of reporting functions or resources between the ISC and ISIC.

120. It should be for Parliament to consider whether:

(a) to retain the system of Prime Ministerial appointment but require the Chair to be a member of a political party not represented in government;

(b) to transfer the ISC's investigative resource in due course to ISIC; and/or

(c) to recast the ISC as a Select Committee (either on its own or merged with the Defence Select Committee) whose members would be elected in the normal way, and to which ISIC would report where necessary in closed session.

TRANSPARENCY

121. It should be recognised that the operation of covert powers is and should remain secret, and that transparency in relation to operational matters is not a realistic goal.

122. Public authorities should however be as open as possible (cf. ISC Report, Recommendation BBB). They should consider how they can better inform Parliament and the public about why they need their powers, how they interpret those powers, the broad ways in which those powers are used and why any additional capabilities might be required. They should contribute to any consultations on the new law, so as to ensure that policy-making is informed by the best evidence.

123. The statistics provided by ISIC should be as informative as possible: the proposals put forward by IOCCO in its December 2014 submission to this Review provide a useful starting point.

124. Both ISIC and the IPT should be as open as possible in their work, and should seek actively to make the public aware of their role as a check on the powers of public authorities.

ANNEXES

Annex 1: LIST OF ACRONYMS (1.24 above)

Below are detailed the acronyms used in this Report.

AAT: Administrative Appeals Tribunal (Australia)

ACPO: Association of Chief Police Officers

ATCSA 2001: Anti-Terrorism Crime and Security Act 2001

ASIO: Australian Security Intelligence Organisation

ASIS: Australian Secret Intelligence Service

CCTV: Closed Circuit Television

CAFT: Corporate Anti-Fraud Team

CEOP: Child Exploitation and Online Protection Centre

CHIS: Covert human intelligence sources

CIU: Communications Intelligence Unit

CJEU: Court of Justice of the European Union

CMA: Competition and Markets Authority

CNE: Computer Network Exploitation

CPS: Crown Prosecution Service

CRASBO: Criminal Anti-Social Behaviour Order

CSE: Communications Security Establishment (Canada)

CSEW: Crime Survey for England and Wales

CSIS: Canadian Security and Intelligence Service

CSPs: Communications Service Providers

CTSA 2015: Counter Terrorism and Security Act 2015

DRIPA 2014: Data Retention and Investigatory Powers Act 2014

DP: Designated Person

DPA 1998: Data Protection Act 1998

DPI: Deep Packet Inspection

DWP: Department for Work and Pensions

ECA 1972: European Communities Act 1972

ECHR: European Convention on Human Rights

ECtHR: European Court of Human Rights

EO 12333: Executive Order 12333 (USA)

EU: European Union

EU Charter: European Union Charter of Fundamental Rights

FBI: Federal Bureau of Investigation (USA)

FISA 1978: Foreign Intelligence Services Act 1978 (USA)

FISC: Foreign Intelligence Surveillance Court (USA)

GCHQ: Government Communications Headquarters

GCSB: Government Communications Security Bureau (New Zealand)

GPS: Global Positioning System

HMRC: Her Majesty's Revenue and Customs

HRA 1998: Human Rights Act 1998

ICCPR: International Covenant on Civil and Political Rights

ICO: Information Commissioner's Office

IGIS: Inspector General of Intelligence and Security (Australia)

IGIS Act: Inspector General of Intelligence and Security Act (Australia)

IMS: IP multimedia sub-system

IMSI: International Mobile Subscriber Identity

IOCA 1985: Interception of Communications Act 1985

IOCC: Interception of Communications Commissioner

IOCCO: Interception of Communications Commissioner's Office

IOT: Internet of Things

ISP: Internet service provider

IP: Internet Protocol

IP address: Internet Protocol address

IPT: Investigatory Powers Tribunal

ISA 1994: Intelligence Services Act 1994

ISA 2001: Intelligence Services Act 2001 (Australia)

ISC: Intelligence and Security Committee of Parliament

ISCommr: Intelligence Services Commissioner

ISIC: Independent Surveillance and Intelligence Commission

ISP: Internet Service Provider

IPT: Investigatory Powers Tribunal

JCDCDB: Joint Committee on the draft Communications Data Bill

JSA 2013: Justice and Security Act 2013

LGA: Local Government Association

LPP: Legal Professional Privilege

MI5: Security Service

MI6: Secret Intelligence Service

MLAT: Mutual Legal Assistance Treaty

MoD: Ministry of Defence

MPS: Metropolitan Police Service

MTIC: Multi-trader intra-community

NAFN: National Anti-Fraud Network

NCND: Neither confirm nor deny

NCA: National Crime Agency

NDA 1985: National Defence Act 1985 (Canada)

NGO: Non-governmental organisation

NSA: National Security Agency (USA)

NTAC: National Technical Assistance Centre

NZSIS: New Zealand Security and Intelligence Service

ONS: Office for National Statistics

OSC: Office of Surveillance Commissioners

OSCT: Office for Security and Counter-Terrorism

OSINT: Open Source Intelligence

OTT: Over The Top (providers)

PACE: Police and Criminal Evidence Act 1984

PCFOC 2014: Protecting Canadians from Online Crime Act 2014 (Canada)

PFA 2012: Protection of Freedoms Act 2012

PGP: Pretty Good Privacy

PIC: Priorities for Intelligence Collection

PRA: Pen Register Act (USA)

PSNI: Police Service of Northern Ireland

RIPA: Regulation of Investigatory Powers Act 2000

RIP(S)A: Regulation of Investigatory Powers (Scotland) Act 2000

RUSI: Royal United Services Institute

SCA: Stored Communications Act 1968 (USA)

SIGINT: Signals Intelligence

SIRC: Security Intelligence Review Committee (Canada)

SISA 1979: Security Intelligence Service Act 1969 (New Zealand)

SOCA: Serious Organised Crime Agency

SPoC: Single Point of Contact

SSA 1989: Security Service Act 1989

SSA 2012: Search and Surveillance Act 2012 (New Zealand)

TA 1984: Telecommunications Act 1984

TEU: Treaty on European Union

THS: Tor Hidden Services

TIA 1979: Telecommunications (Interception and Access) Act 1979 (Australia)

TICSA 2013: Telecommunications (Interception Capability and Security) Act 2013 (New Zealand)

Tor: The Onion Router

url: Uniform Resource Locator

VOIP: Voice Over Internet Protocol

VPN: Virtual Private Networks

WA 1968: Wiretap Act 1968

WGD: Warrant Granting Department

WTA 2006: Wireless Telegraphy Act 2006

Annex 2: DEFINED TERMS (1.24 above)

Below are listed the terms defined for ease of reference and used in this Report.

1. **Acquisition Code** (Acquisition and Disclosure of Communications Data Code of Practice, March 2015).

2. **Belhadj IPT Case** (*Belhadj and others v the Security Service and others* (Case No IPT/13132-9/H)).

3. **Big Data** (very large data sets).

4. **Charles Farr Statement** (Charles Farr's witness statement of 2014 in the Liberty IPT Case).

5. **Content-derived metadata** (the technical and "less intrusive" elements of communications content)

6. **Covert Surveillance and Property Interference Code** (Covert Surveillance and Property Interference Code of Practice, December 2014).

7. **Data Protection Directive** (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data)

8. ***Digital Rights Ireland*** (Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* and *Seitlinger and others*, EU:C:2014:238).

9. **Draft Equipment Interference Code** (Draft Equipment Interference Code of Practice, February 2015).

10. **Draft Interception Code** (Draft Interception of Communications Code of Practice, February 2015).

11. **e-privacy Directive** (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector)

12. **EU Data Retention Directive** (Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC**).**

13. **Interception Code** (Interception of Communications Code of Practice).

14. **ISC Privacy and Security Report** (Intelligence and Security Committee, *Privacy and Security: A modern and transparent legal framework*, HC 1075, (March 2015)).

15. **ISC Rigby Report** (Intelligence and Security Committee, *Report on the Intelligence relating to the murder of Lee Rigby*, (November 2014)).

16. **JCDCDB Report** (Report of the Joint Committee on the Draft Communications Data

Bill, HL Paper 79 HC 479 (December 2012)).

17. **Liberty IPT Case** (*Liberty and others v The Secretary of State for Foreign and Commonwealth Affairs and others*, Case Nos. IPT/13/77/CH; 13/92/CH; 13/194/C and 13/204/CH, [2015] UKIPTrib 13_77-H).

18. **Liberty ECtHR Application** (*10 Human Rights Organisations v United Kingdom,* an application to the ECtHR filed on 10 April 2015).

19. **PI IPT Case** (*Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ and others*, Case No. IPT/14/85/CH).

20. **Retention Code** (Retention of Communications Data Code of Practice, March 2015).

21. **The RUSI Review** (Independent Surveillance Review of the Royal United Services Institute).

22. **Service providers** (used to refer to: (1) companies which offer communications services (Communications Service Providers properly so called), such as BT and Vodafone, (2) companies providing internet access (commonly referred to as Internet Service Providers), such as AOL, Virgin Media and Sky (collectively, technical readers will know these two categories as the four lower levels of the OSI 7-layer model), and (3) companies which operate "*over the top*" of an internet connection (commonly called OTT providers or Applications Services Providers), such as Facebook and Twitter).

23. **The Snowden Documents** (documents stolen from the US National Security Agency by the contractor Edward Snowden, and published since 2013, purporting to describe various surveillance capabilities and activities).

24. **SURVEILLE Report** (SURVEILLE, *Paper Assessing Surveillance in the Context of Preventing a Terrorist Act,* (May 2015)).

25. **Venice Commission Report** 5 (European Commission for Democracy Through Law (Venice Commission), *Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies*, Study No 719/2013 (April 2015)).

Annex 3: WRITTEN SUBMISSIONS RECEIVED **(1.21 above)**

Access
All Party Parliamentary Group on Drones
Association of Chief Police Officers
The Bar Council
Dr Paul Bernal
Big Brother Watch
Bingham Centre for the Rule of Law
Birnberg Peirce and Partners
Caspar Bowden
BT
Center for Technology & Democracy
Jan Clements
Competition and Markets Authority
Paul Connolly
Dr Andrew Defty and Professor Hugh Bochel
Demos
DWP
Mark Dzięcielewski
EE
Equality and Human Rights Commission
Facebook/Google/Microsoft/Twitter/Yahoo
Faculty of Advocates
Gambling Commission
Peter Gill
Global Network Initiative
GCHQ
Richard Greenhill
Guardian Media Group
Morton Halperin
The Henry Jackson Society
HMRC
Home Office
Human Rights Watch
Interception of Communications Commissioner's Office
The Internet Services Providers' Association
The Internet Telephony Services Providers' Association
The Law Society
Liberty
Local Government Association
Ray McClure
Media Lawyers Association
Metropolitan Police Service
MI5
MI6
Gavin Millar QC
National Union of Journalists

NCA
The Newspaper Society
Ofcom
Sir David Omand
Open Rights Group
Police Scotland
PSNI
Charles Raab
Rights Watch (UK)
Roke Manor Research Ltd
Royal Mail
The Scottish Government
Graham Smith
The Society of Editors
Professor Peter Sommer
Talk Talk Group
Telefonica
Three
UCL
Virgin Media
Vodafone

Annex 4: MEETINGS (1.21 above)

UNITED KINGDOM

Rt Hon Theresa May MP, Home Secretary
Rt Hon Yvette Cooper MP, Shadow Home Secretary
James Brokenshire MP, Security Minister
Office of Security and Counter-Terrorism, Home Office
Foreign and Commonwealth Office
Sir Nigel Sheinwald, Special Envoy on intelligence and law enforcement data sharing

MI5
MI6
GCHQ
National Technical Assistance Centre

US Embassy
Canadian High Commission
German Embassy

Alison Saunders, Director of Public Prosecutions
Crown Prosecution Service

National Crime Agency
Rob Wainwright, Director, Europol
National Policing Lead for Communications Data
Metropolitan Police Commissioner
MPS Assistant Commissioner for Specialist Crime and Operations
MPS Communications Intelligence Unit
MPS SO15 Communications Data Team
Senior National Coordinator, Counter-Terrorism
Data Communications Group Futures
Chief Constable and Deputy Chief Constable, Police Service of Northern Ireland
Gloucestershire Constabulary
Nottinghamshire Police
Local Government Association
Association of Chief Trading Standards Officers
Hampshire Trading Standards
Brighton City Council
National Anti-Fraud Network

Members of Intelligence and Security Committee, UK Parliament
Members of Joint Committee on Human Rights, UK Parliament

Sir Michael Burton, President, Investigatory Powers Tribunal
Charles Flint QC, Member, Investigatory Powers Tribunal
Rt Hon Sir Mark Waller, Intelligence Services Commissioner

Rt Hon Sir Paul Kennedy, Acting Interception of Communications Commissioner
Rt Hon Sir Anthony May, Interception of Communications Commissioner
Rt Hon Sir Christopher Rose, Chief Surveillance Commissioner
Rt Hon Lord Judge, Chief Surveillance Commissioner designate
Rt Hon Sir William Gage and Rt Hon Sir Scott Baker, Office of Surveillance Commissioners
Sue Cobb, Chief of Staff to the Intelligence Services Commissioner
Jo Cavan, Head of IOCCO
Dr Michael Maguire, Police Ombudsman for Northern Ireland

Royal United Services Institute
Open Society Justice Initiative
Jamie Bartlett and Carl Miller, Demos
Eric King, Privacy International
Alan Rusbridger and staff, The Guardian
Prof Ian Brown, University of Oxford
Dr Richard Clayton, University of Cambridge

Dinah Rose QC
Matthew Ryder QC
Martin Chamberlain QC
Jonathan Glasson QC
Tom Hickman
Ben Jaffey

Sir David Omand
Graham Smith
Morton Halperin

Apple
BT
Facebook
Google
Vodafone
Communications Data Strategy Group, CSP representatives

GERMANY

Federal Ministry of the Interior
Federal Ministry of Justice
Federal Chancellery
Federal Data Protection Authority
BND (foreign intelligence agency)
BfV (internal security service)
Federal Office for the Protection of the Constitution
G10 Commission
Bitkom (Federal Association for Information Technology)
Prof Christoph Moellers, Humboldt University of Berlin

Prof Hans-Georg Albrecht, Max Planck Institut

UNITED STATES

Office of the Director of National Intelligence
National Security Agency
Federal Bureau of Investigation
Department of Justice

Foreign Intelligence Surveillance Court

Yahoo
Google
Apple
LinkedIn
Dropbox
Twitter

Susan Friewald, University of San Francisco
David Medine and Prof Jim Dempsey, PCLOB
Prof David Cole and Alberto Bedoya, Georgetown University

Access
American Civil Liberties Union
Cato Institute
Center for Democracy and Technology
Center for National Security Studies
Electronic Frontier Foundation
Human Rights Watch
New America Foundation
Third Way

CANADA

Office of the Communications Security Establishment Commissioner
Security Intelligence Review Committee
Chief Justice and Justices of the Federal Court
Justice Canada
Royal Canadian Mounted Police
Public Prosecution Service of Canada
Professor Craig Forcese, University of Ottawa

BRUSSELS

Paul Nemitz, DG Justice, Director Fundamental Rights
Luigi Soreca, DG Home, Director Internal Security
Matthias Reute, DG Home, Director General
Gilles de Kerkhove, Counter-Terrorism Coordinator
Stefano Manservisi, Chef de Cabinet of High Representative Mogherini
Giovanni Buttarelli, European Data Protection Supervisor
Claude Moraes MEP, Chair of LIBE Committee
Timothy Kirkhope MEP
Axel Voss MEP
Marju Lauristin MEP

Not in that list are the Review team (1.23 above), the people with whom I enjoyed fruitful dialogues at various conferences, notably those organised by Wilton Park in October and November 2014, those referred to at 8.39 above whom I did not meet but who gave their assistance with the law of the Five Eyes countries, and those whose assistance came via email or twitter.

I am also grateful to Simon McKay for letting me see proofs of his *Covert policing: law and practice* (2nd edn. 2015), to Poppy Anderson for Viscount Falkland (2.20(a) above), to Cian Murphy and, as ever, to my special adviser Professor Clive Walker.

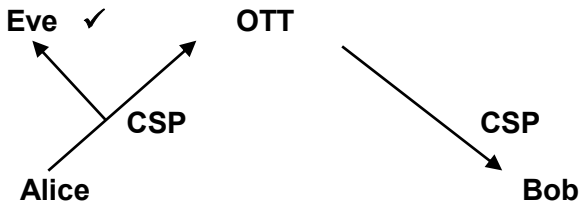
Annex 5: IMPACT OF ENCRYPTION AND ANONYMISATION

(4.61 above)

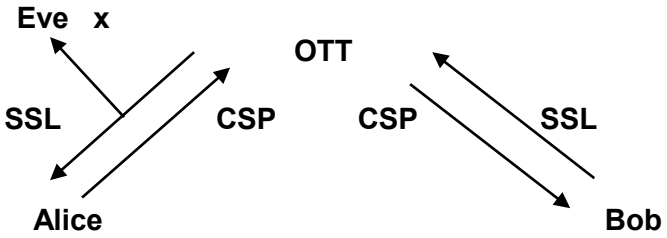
1. In this Annex the following key is used:

   (a) Eve: Agency.
   (b) Alice: Sender of email.
   (c) Bob: Recipient of email.
   (d) SSL: Secure Sockets Layer.
   (e) The communications data being discussed in the following examples is sender/recipient details.

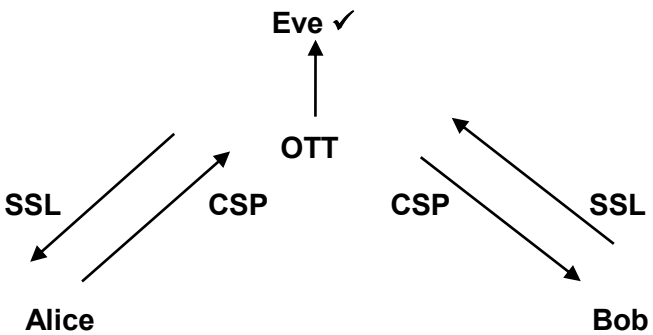
2. First example: there is no encryption in use. Eve can obtain access to the content and sender/recipient details of an email sent by Alice to Bob via the CSP.



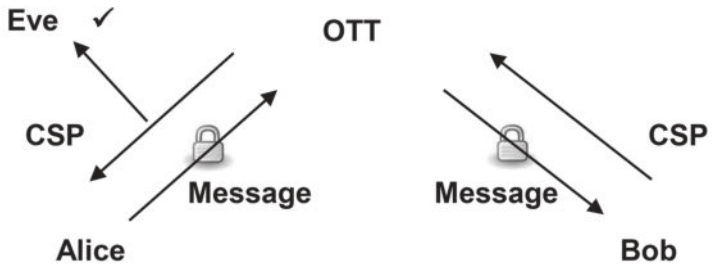
3. Second example: the OTT provider is using SSL, meaning that the content and sender/recipient details of an email sent by Alice to Bob are visible to the OTT. They are not visible to the CSP. The CSP is only able to see that the email is to be sent to the particular OTT provider.



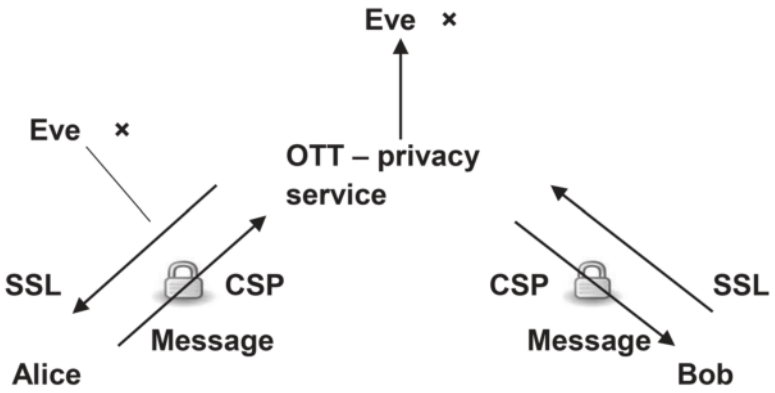
4. Third example: Eve can access the content and sender/recipient details from the OTT provider via a warrant or court order. If the OTT provider is based overseas, it may not cooperate with a UK court order.



5. Fourth example: the use of end-to-end encryption means that the content of the email is not visible to the CSP or the OTT provider. Sender/recipient details are visible to both.



6. Fifth example: the OTT provider is a privacy service. It does not retain data at all and so cannot provide data in response to a warrant or court order. If the OTT provider does collect data, Alice and Bob can hide sender/recipient details by using an anonymisation service such as Tor and end-to-end encryption will provide protection for the content. Content and sender/recipient details are not visible to a CSP because SSL and end-to-end encryption are used. The privacy service could be compromised overtly or covertly and so a user may use an anonymisation service before visiting the privacy service.



7. For the sake of completeness, it should be noted that the combined protection offered by SSL, end-to-end encryption and anonymisation services is not absolute. A user of all three is still vulnerable to CNE.

Annex 6: LIST OF BODIES WITH NON-RIPA POWERS (6.18 above)

Department	Mechanisms (non-RIPA)	Section
Department for Business Innovation and Skills	Business Protection from Misleading Marketing Regulations 2008	21 (1) , 23(1)
	Companies Act 1985	434 (2); 444 (1); 447 (2) (3)
	Consumer Credit Acts 1974, 1985	36B (1), 162, 174A
	Consumer Protection Act 1987	18 (1), (2); 29(4)(5)(6)
	Consumer Protection from Unfair Trading Regulations 2008	21(1)(b)(d)
	Copyright Design and Patents Act 1974	16(a)
	Copyright Design and Patents Act 1988	107A (2), 198A (2)
	Enterprise Act 2002	225-227
Competition & Markets Authority	Companies Act 1985	434 (2); 444 (1); 447 (2) (3)
	Competition Act 1998	
	Enterprise Act 2002 (Soon to be replaced by the Consumer Rights Bill)	225-227
	Consumer Credit Act 1974	
	Business Protection from Misleading Marketing Regulations 2008	21, 23
	Fair Trading Acts 1973, 1986	29(1)
Financial Conduct Authority	Consumer Credit Acts 1974, 1985	36B (1), 162, 174A
	Financial Services & Markets Act 2000	16(1)(2), 131E(1), 165, 165A, 171-175, 218A-221, 305
	Pensions Act 2004	75, 192
	Pensions (Northern Ireland) Order 2005	67,68 & 73
	Merchant Shipping (Accident Reporting and Investigative) Regulations 2005	12(?)
Ministry of Justice	Prison Rule 35	

Department for Work and Pensions	Pensions Act 2004	75, 192
	Pensions (Northern Ireland) Order 2005	67,68 & 73
	Social Security Administration Act 1992, as amended by the Social Security Fraud Act 2001	09B and 110A
	Social Security Administration Act 1992, as amended by the Social Security Fraud Act 2001 (Northern Ireland)	110(6)
	Child Support Act 1991	15(6)
Northern Ireland Department of Social Development	Child Support (Northern Ireland) Order 1991	16, 17
Northern Ireland Department of Agricultural and Rural Development	Animal Health Act 1981 amended by the Disease of Animals (Northern Ireland) Act 2010	36(i) (5)
DEFRA	Animal Health Act 1981	36(i) (5)
HMRC	Finance Act 1988	127
	Taxes Management Act 1970	20(1)
	Value Added Tax Acts 1983, 1994	Schedule 11 Section 4
Scottish Government	Adult Support & Protection (Scotland) Act 2007	10(1), 61
Welsh Government	Environmental Protection Act 1990	19(2), 71(2), 116(1)
Northern Ireland Department of Enterprise Trade & Investment	Business Protection from Misleading Marketing Regulations 2008	21(1), 23(1)
	Consumer Credit Acts 1974 and 1985	36B(1), 162, 174A
	Consumer Protection from Unfair Trading Regulations 2008	21(1)(b)(d)
	Timeshare Act 1992	Schedule 2 s3(1)(2)
	Trade Marks Act 1994	93(2)
	Video Recordings Act 2010	17(2)
	Weights and Measures (Northern Ireland) Order 1981	41(2) Schedule 9(4)

	Control of Pollution Acts 1974, 1975	93(1)
	Environmental Protection Act 1990	19(2), 71(2), 116(1)
	Salmon & Freshwater Fisheries Act 1975	31(?)
General Dental Council	Dentists Act 1984 (Amendment) Order 2001 or 2005	50(3)
Police, National Crime Agency, Police Service of Northern Ireland	Dangerous Dogs Act 1991	5(2)
	Drug Trafficking Act 1985	55
	Police and Criminal Evidence Act 1984	19, 20
	Serious Organised Crime and Police Act 2005	66
	Video Recordings Act 1984, 2010	17(2)
	Terrorism Act 2006	33
Department for Transport (Marine Accident Investigation Boards)	Merchant Shipping Act 1995	257-259
Department for Transport (Maritime and Coastguard Agency)	Merchant Shipping Act 1995	257-259
	Merchant Shipping (Accident Reporting and Investigative) Regulations 2005	12(?)
Home Office (Border Force)	Immigration Act 1971	28D
	Immigration and Asylum Act 1999	127, 131
Ministry of Justice (National Offender Management Service)	Prison Rule 35	35
Scottish Criminal Casework Review Commission	Criminal Procedure (Scotland) Act 1995	194L
Gangmasters Licensing Authority	Gangmasters (Licensing) Act 2004	16
Information Commissioner's Office	Privacy and Electronic Communications Regulations 2003 (as amended 2011)	31A
	Enterprise Act 2002	225-227
	Data Protection Act 1998	29 (3), Schedule 9(1)(3)

Ofcom	Communications Act 2003	135
	Enterprise Act 2002	225-227
	Wireless Telegraphy Act 2006	89(4), 99(3)
	Postal Service Act 2011	55
Scottish Fire and Rescue	Fire Precautions Act 1971	19(1)
Northern Ireland Fire Authority	The Fire and Rescue Services (Northern Ireland) Order 2006	19(1)
England Fire Authority	Fire Precautions Act 1971	19(1)
Welsh Fire Authority	Fire Precautions Act 1971	19(1)
Northern Ireland Prison Service	Prison Rule 35	35
Local Authorities	Business Protection from Misleading Marketing Regulations 2008	21 (1) , 23(1)
	Consumer Credit Acts 1974, 1985	36B (1), 162, 174A
	Consumer Protection Act 1987	18 (1), (2); 29(4)(5)(6)
	Consumer Protection from Unfair Trading Regulations 2008	21(1)(b)(d)
	Control of Pollution Acts 1974, 1975	93(1)
	Copyright Design and Patents Act 1974	16(a)
	Copyright Design and Patents Act 1988	107A (2), 198A (2)
	Dangerous Dogs Act 1991	5(2)
	Fire Precautions Act 1971	19(1)
	Food Safety Act 1990	32(5)(6)
	Local Government Act 1971, 1974 and 1982	141
	Package Travel, Package holiday and Tours Act 1992	Schedule 3 Section 3
	Property Misdescriptions Act 1991	Schedule s3(1)
	Timeshare Act 1992	Schedule 2 s3(1)(2)

	Trade Descriptions Act 1968	28(1)
	Trade Marks Act 1938, 1994	93(2)
	Weights and Measures Act 1985	39, 79(2), Schedule 8(4)
	Weights and Measures (Northern Ireland) Order 1981	41(2), Schedule 9(4)
Charity Commission	Charities Act 2011	47, 52
Charity Commission for Northern Ireland	Charities Act (Northern Ireland) 2008	22 (3), 23 (1)
Environment Agency (and regional equivalents)	Control of Pollution Acts 1974, 1975	93(1)
	Environmental Protection Act 1990	19(2), 71(2), 116(1)
	Salmon & Freshwater Fisheries Act 1975	31(?)
	Environment Act 1995	108(4)(k)
Food Standards Agency	Food Safety Act 1990	32(5)(6)
Health and Safety Executive	Regulatory Reform (Fire Safety) Order 2005 in England and Wales Fire (Scotland) Act 2005 (FSA) in Scotland	19(1)
	Health and Safety at Work Act 1974	20
	Working Time Regulations 1998	Reg. 28(7) and Schedule 3
	Food and Environment Protection Act 1985	Part III s19 and Schedule 2, para 2.
	Plant Protection Products Regulations 2011	Reg. 7 and Schedule 1, para 4
	Plant Protection Products (Sustainable Use) Regulations 2012	Reg. 20 and Schedule 3, para 4

	Environmental Protection Act 1990	115
	Regulatory Reform (Fire Safety) Order 2005	Article 26
	Fire (Scotland) Act 2005	62
	Electricity Act 1989	28, 30
	Electricity Safety, Quality and Continuity Regulations 2002 REACH Enforcement Regulations 2008	Reg. 30. Schedule 6
Pensions Regulator	Pensions Act 2004	75, 192
	Pensions (Northern Ireland) Order 2005	67,68 and 73
British Board of Film Classification	Video Recordings Act 1984, 2010	17(2)
General Optical Council	Opticians Act 1989	21(1), (3)
Child Support Agency	Child Support Act 1991	15(6)
UKBA (See Home Office)	Immigration and Asylum Act 1999	127, 131
General Pharmaceutical Council (for the Royal Pharmaceutical Society of Great Britain)	Pharmacy Order 2010	11
Intellectual Property Office	Copyright Design and Patents Act 1974, section	16(a)
	Copyright Design and Patents Act 1988, sections	107A (2); 198A (2)
Department for Culture, Media and Sport	Privacy and Electronic Communications Regulations 2003	

Trading Standards	Business Protection from Misleading Marketing Regulations 2008	21 (1) , 23(1)
	Companies Act 1985	434 (2); 444 (1); 447 (2) (3)
	Consumer Credit Acts 1974, 1985	36B (1), 162, 174A
	Consumer Protection Act 1987	18 (1), (2); 29(4)(5)(6)
	Consumer Protection from Unfair Trading Regulations 2008	21(1)(b)(d)
	Copyright Design and Patents Act 1974	16(a)
	Copyright Design and Patents Act 1988	107A (2), 198A (2)
	Enterprise Act 2002	225-227

Annex 7: THE SNOWDEN ALLEGATIONS (7.7 above)

1. In this annex, I summarise some of the main allegations that emerge from the Snowden Documents unlawfully taken from the NSA in the United States and subsequently published by a number of newspapers.[1]

2. As emphasised at para 7.7 of the Report, this summary should not be taken as any endorsement by me of the truthfulness or representative nature of the practices alleged (all of which, save PRISM, are neither confirmed nor denied by the Government), nor of the conduct of Edward Snowden.

Bulk interception allegations

PRISM

3. The PRISM programme was said to involve the collection by the NSA of data from the servers of nine US internet companies (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple - "*the Prism Providers*"). Types of data collected included a range of digital information such as email, chat, videos, photos, stored data, VOIP, video conferencing and online social networking details. An automated system called PRINTAURA organised the data by category. Some providers had the capability to provide real-time notification of an email event by a target, such as a log-in.[2]

UPSTREAM

4. UPSTREAM data collection programmes such as BLARNEY, OAKSTAR, FAIRVIEW and STORMBREW, were said to involve the collection by the NSA of communications from the infrastructure which carries internet traffic*,* rather than from the servers of internet companies. A slide referring to UPSTREAM programmes is said to describe "*the collection of communications from fiber cables and infrastructure as data flows by*".[3]

TEMPORA

5. This programme was said to involve the interception by GCHQ of digital traffic flowing through the underwater fibre optic cables landing in the UK. It is described as providing analysts access to "*huge amounts of data*". "*All web, email, social, chat, EA, VPN, VOIP*" is said to be "*promote*" from the cables; "*high-volume, low value traffic*", such as peer-to-peer downloads is then filtered out. A buffering technique holds data in a "*repository*"; content for three days and metadata for up to 30 days "*to allow retrospective analysis and forwarding to other systems*". Search terms are applied to the promoted data and any hits are entered into TEMPORA. Data is also entered into TEMPORA based on "*technology type or IP subnet*". In 2012, GCHQ appeared to be managing to collect data from 46 cables in this way.[4]

---

1 References in this Annex are to on-line versions of the documents discussed.

2 https://www.eff.org/document/2013-06-06-wapo-prism.
https://www.eff.org/document/20140430-intercept-prism-olympics.

3 https://www.eff.org/document/2013-06-08-guard-prism.

4 https://www.eff.org/document/20140618-der-spiegel-gchq-report-technical-abilities-tempora.

MUSCULAR

6. The MUSCULAR programme was said to be a joint GCHQ and NSA project which intercepted internal fibre optic cables used by Google and Yahoo, to transmit unencrypted data between their data centres.[5] During a 30-day period in 2012-2013 it was said that 181 million records were sent from a British collection point back to the USA via this programme.[6]

DISHFIRE

7. Slides relating to this programme describe the collection of almost 200 million text messages per day in 2011 by NSA from around the world. Slide 5 describes why SMS is regarded as so useful**;** they contain metadata and "*metacontent*" (content derived metadata), the latter includes such "*gems*" as notifications relating to credit card transactions and flight plans which can enhance analytics.[7]

OPTIC NERVE

8. Under this programme Yahoo webcam images were said to be intercepted by GCHQ. In one 6 month period in 2008 images were collected from 1.8 million Yahoo user accounts globally. The programme saved one image every five seconds and users were "*unselected",* i.e., the collection was in bulk rather than targeted. Between 3% and 11% of images were said to involve "*undesirable nudity*". This programme was also used to trial facial recognition technology.[8]

MYSTIC and RETRO

9. The NSA programme referred to as MYSTIC was described as a voice interception programme which used buffering to record an entire country's telephone calls and enable access for a month after the call took place. The RETRO tool, short for *retrospective retrieval*, was said to enable the retrieval of calls up to thirty days in the past.[9]

Bulk Processing tools

10. Under the FASCIA programme the NSA was said to track the movements of mobile phones by collecting location data as people move around. Almost 5 billion mobile phone location records were logged per day.

11. A data sorting tool called CO-TRAVELER was said to look for unknown associates of known intelligence targets by tracking people whose movements intersect.[10]

12. PREFER was said to be the analytic tool used to carry out analysis of the text messages collected via the DISHFIRE programme outlined above. It was able to

---

5 https://www.eff.org/document/2013-10-30-wapo-muscular-smiley
https://www.eff.org/document/2013-10-30-wapo-muscular.

6 https://www.eff.org/document/2013-11-04-wapo-windstop.
https://www.eff.org/document/2013-11-04-wapo-sso-overview.

7 https://www.eff.org/document/20140116-guard-dishfire-presentation.

8 https://www.eff.org/document/20140227-guard-gchq-optic-nerve.

9 https://www.eff.org/document/20140318-wapo-description-data-collection-under-mystic.
https://www.eff.org/document/20140318-wapo-adding-another-country-mystic-program.

10 https://www.eff.org/document/20131210-wapo-cotraveler-overview.

extract information from missed call alerts or texts with international roaming charges. Missed call alerts could allow contact chaining, i.e., working out someone's social network. Border crossings could be worked out from roaming charges texts and names could be extracted from electronic business cards.

13. The XKEYSCORE system was said to be developed by the NSA, to allow analysts to carry out a search, using a single search term, such as an email address, or telephone number, across three days worth of raw data collected via a number of programmes such as PRISM and UPSTREAM. According to documents relating to OPTIC NERVE, the webcam material collected via this programme was fed into XKEYSCORE. XKEYSCORE indexed data sources including email addresses, IP addresses, port numbers, file names, cookies and buddy-lists. Monitoring of Facebook chats was said to be possible simply by entering a Facebook user name and date range. A slide labelled "*future"* listed VOIP as a target. Another slide described how 300 terrorists were captured using intelligence generated from XKEYSCORE.[11]

14. DEEP DIVE was said to have a greater capability than traditional XKEYSCORE which handles low rates of data and ingests all of it. DEEP DIVE could handle 10 gigabytes of data. It "*promoted"* data that has a "*potential intelligence value"* and only that is ingested into XKEYSCORE. Data "*that is not allowed to be in the system – UK-UK"* is blocked. DEEP DIVE XKEYSCORE was said to be used by the TEMPORA programme though this was not the only way in which data was promoted to TEMPORA. Promotion also took place based simply on technology type or IP subnet.[12]

Computer Network Exploitation

15. Documents referred to a number of programmes aimed at "*Active SIGINT*" or CNE. They were said to involve implanting malware (software designed to disrupt a computer) directly onto a user's computer. Examples in the documents describing the use of this technique by GCHQ included a programme called NOSEY SMURF which involved implanting malware to activate the microphone on smart phones, DREAMY SMURF, which had the capability to switch on smart phones, TRACKER SMURF which had the capability to provide the location of a target's smart phone with high-precision, and PARANOID SMURF which ensured malware remained hidden.[13]

16. It was also said that a GCHQ project called OPERATION SOCIALIST used technology called QUANTUMINSERT to direct staff at Belgacom, without their knowledge, to fake websites in order to plant malware on their computers.[14] GCHQ was also said to have gained access via CNE to the entire network of a company called Gemalto, which produces SIM cards, including their encryption keys.[15]

17. Documents also said that implants of malware can take place in bulk. An automated system called TURBINE, allows "*the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by*

11 https://www.eff.org/document/2013-07-31-guard-xkeyscore-training-slides.
12 *Ibid.*
13 https://www.eff.org/document/20140128-guard-leaky-phone-apps.
14 https://www.eff.org/document/2013-09-20-spiegel-belgacom.
15 https://www.eff.org/document/20150219-intercept-sim-card-encryption-key-theft-and-mobile-network-access.

groups instead of individually."[16]

18. OPERATION MULLENIZE was said to involve a technique called User Agent Staining to write a unique mark or "*stain*" onto a target machine. The unique marker enabled all the events from the machine to be pieced together to "*recreate a browsing session."* The catalyst for the operation was said to be the sharing of an IP address by many users at one time, which made it difficult to identify users. It was said that a method has been devised to enable "*staining"* on a "*large-scale*".[17]

16 https://www.eff.org/document/20140315-intercept-turbine-intelligence-command-and-control.
17 https://www.eff.org/document/20131004-wapo-gchq-mullenize.

Annex 8: INTERCEPTION CASE STUDIES (7.18 above)

Case 1

1. A criminal investigation into a UK-based organised crime group involved in the importation of Class A drugs from South America.

2. Interception assisted in identifying the command and control structure of the group and their associates in other European countries. It identified individuals responsible for facilitating the supply of drugs and also those involved in establishing front companies for importing legal goods. Intercept provided intelligence on the modus operandi employed by the group, the dates and location of the importation, and the storage place of a series of drug shipments.

3. This resulted in the arrest of UK-based members of the group and their co- conspirators overseas, as well as the seizure of significant quantities of Class 'A' drugs, foreign currency, firearms and ammunition. Intercept material provided key intelligence which was pivotal in building an evidential case and ended in the successful prosecution of the defendants. It also served to enhance the Serious Organised Crime Agency **[SOCA]**[18]'s working relationships with overseas partners involved in the investigation.

Case 2

4. A criminal investigation into an organised crime group based in the south east of England involved in acquiring, supplying, and storing firearms in the UK.

5. Interception provided intelligence on the structure of the organised crime group, its methods of working, and the types of crime it was involved in. It helped to identify the types of firearm and the locations where the weapons and ammunition were stored. This led to the seizure of weaponry which ranged from handguns to automatic weapons, as well as significant quantities of ammunition. It also provided intelligence on turf wars with other groups operating in the area, which was critical to operational planning.

6. The intelligence provided by intercept was developed further and helped to identify those responsible for the wholesale supply of firearms in Europe. It also revealed changes to the structure of the group and its weaknesses, enabling SOCA to re- focus the investigation.

7. The result was the successful prosecution of a significant number of gang members involved in the supply and distribution of firearms.

Case 3

8. A criminal investigation into a pattern of escalating violence between a number of rival organised crime groups, including street gangs linked to the London drug economy, operating across the capital.

---

[18] Now replaced by the NCA.

9. Intelligence derived from interception indicated a conflict between organised crime groups as each sought to control a greater section of the drugs market. The intelligence suggested the use of firearms by the groups. This prompted immediate steps to tackle the group, with the intention of dismantling the network, disrupting the supply of Class A drugs, preventing further loss of life and arresting those involved. The operation also targeted individuals directly involved in gun possession and crime whilst disrupting other criminal activities such as small-scale drug dealing, acquisitive crime and serious assaults.

10. Intercepted material identified the individual co-ordinating the sale of significant amounts of Class A drugs, led to the location of his safe storage premises, and identified senior gang members involved in the supply chain. It also enabled junior gang members to be identified as couriers of the drugs to numerous locations across London, the Home Counties and beyond, including the method and timing transport. Interception also revealed that the head of the organised crime group was conspiring with others to shoot a rival. This led to an armed stop of the target whilst he was *en route* to the hit location. He was found to be in possession of a loaded firearm and arrested.

11. The primary operation led to the collapse of the network operating across London and the Home Counties. During the course of the operation, intelligence from interception led to the seizure of over 40 firearms, in excess of 200kg of Class A drugs, the seizure of over £500,000 of cash and over 100 arrests.

Case 4

12. A criminal investigation into a London-based money laundering network, linked to several organised crime groups that were responsible for a major share of criminal activity across London.

13. An operation was launched in partnership with HMRC to identify the proceeds linked to the groups' criminal activities and to deny them funds. The police had identified that a considerable quantity of cash was being laundered on a regular basis by a relatively small group of criminals. Launderers were identified as working for multiple crime networks and making significant profits. However, traditional policing methods were unable to provide details of how the network ran their business.

14. Intercepted material indicated the method by which the laundering network was moving funds between accounts. This led to the covert interception of high value cash transactions, depriving the organised crime groups of their profits and diminishing their ability to complete criminal transactions.

15. During the operation, cash in excess of £3 million was seized. Intercept intelligence indicated that a number of criminal enterprises had collapsed and a number of targets had been forced to cease their activities due to a lack of funding.

Case 5

16. Multi-trader intra-community **[MTIC]** fraud is estimated to cost the exchequer approximately £750 million annually. The fraud typically comprises a scheme involving a number of participants which is set up with the sole purpose of defrauding the public purse. For example, an organised crime group acquires a VAT registration number in the UK for the purposes of purchasing goods free from VAT in another EU member state. The goods are imported into the UK and sold at a VAT inclusive price. The UK company selling the goods will then "*go missing*" without paying the output tax due to HMRC. The criminally obtained funds will be laundered through a complex network of financial transactions involving bank transfers and cash movements in the UK and overseas. In practice, MTIC fraud will involve complex layers of companies performing different functions in an effort to conceal the fraud and to thwart investigation and compliance activity.

17. In one particular operation, supported by interception, a total of £3.2 billion in VAT repayments was withheld from criminal groups fraudulently trading in mobile telephones and computer chips. Interception was also critical in identifying the bank of first choice for laundering the proceeds of the crimes. Working with international partners, HMRC was able to prevent the distribution of assets to the criminal gangs. The scale of the criminal conspiracy and related laundering operation is illustrated by the fact that over $200 million of MTIC funds have been frozen and are the subject of criminal and civil action.

18. Since HMRC started using interception to support investigations into MTIC fraud, the level of attempted fraud has reduced substantially from an estimated high of £5 billion in 2005/2006 to an estimated current figure of £750 million.

Annex 9: BULK DATA CASE STUDIES (7.27 above)

Case Study 1

1. Since HMRC started using interception to support investigations into MTIC fraud, the level of attempted fraud has reduced substantially from an estimated high of £5 billion in 2005/2006 to an estimated current figure of £750 million.

2. In the late 2000s, bulk data enabled GCHQ to trigger a manhunt for a known terrorist linked to previous attacks on UK citizens. At a time when other intelligence sources had gone cold, GCHQ was able to pick up the trail by identifying patterns of activity online believed to be unique to the suspect. Follow-up searches of bulk data provided further leads for the investigation. This work in turn highlighted links to extremists in the UK. Through a series of arrests, the network was successfully disrupted before any attack could place.

Case study 2

3. In 2010 GCHQ analysts identified an airline worker in the UK with links to al-Qaida. Working with the police, agencies investigated the man, who it transpired had offered to use his access to the airport to launch a terrorist attack from the UK, and pieced together the evidence needed to successfully convict him. This individual had taken great care to ensure that his extremist views and plans were totally concealed in his offline behaviour, meaning that this investigation and conviction would have been highly unlikely without access to bulk data.

Case study 3

4. Sometimes, because of the international nature of al-Qaida inspired terrorism, bulk data is the first and last line of defence. In 2010, an intelligence operation identified a plot which came right from the top of al-Qaida: to send out waves of operatives to Europe to act as sleeper cells and prepare waves of attacks. The intelligence specified unique and distinctive communications methods that would be used by these operatives. GCHQ, in partnership with many other countries, was able to identify operatives by querying bulk data collection for these distinctive patterns. This international effort led, over a period of months, to the arrest of operatives in several European countries at various stages of attack preparation – including one group literally *en route* to conducting a murderous attack.

Case study 4

5. In April 2011, GCHQ intelligence uncovered a network of extremists in the UK who had travelled to Pakistan for extremist training. Whilst the targets were abroad, GCHQ analysis revealed that the group had made contact with al-Qaida. When the group returned to the UK, intelligence suggested that they aspired to conduct an attack, possibly using Improvised Explosive Devices (IEDs). In April 2012, the group was arrested and later charged (in April 2013) under Terrorism Act 2006 s5, for which they received sentences ranging from 5-16 years in prison.

Case study 5

6. GCHQ used analysis of bulk data to track down two men overseas who had been harnessing the vulnerabilities of the web to blackmail hundreds of children across the world, including the UK, into exposing themselves online – causing them huge trauma. Some of the victims self-harmed and considered suicide. It was the vital work of GCHQ analysts that brought this abuse to an end: they were able to confirm the suspects' names and locations, and to identify an accomplice. After liaison between law enforcement agencies, the two men were arrested and jailed in their home country.

Case study 6

7. 2014 bulk data analysis of known ISIL extremists in Syria highlighted links to an unidentified individual whose contacts, locations and attempts to hide his internet activity raised analysts' suspicions. This analysis of bulk data provided the trigger for an investigation involving many different agencies across several countries. This investigation quickly led to the suspect's arrest and prevented a bomb plot in mainland Europe which was materially ready to proceed.

Annex 10: UK RETAINED COMMUNICATIONS DATA USE CASES

(7.49 above, European Commission)

Case 1

1. In September 2009 the body of taxi driver Stuart Ludlam was discovered with two gunshot wounds to the head in the boot of his taxi outside the train station in Derbyshire Police carried out checks on the mobiles Ludlam was carrying at the time of his murder in order to help identify his killer. His work telephone had been stolen but data on communications using that device were identified through subscriber checks which revealed that Ludlam had received diverted calls from the main taxi office number. Incoming and outgoing call data with cell site locations were requested to trace Ludlam's movements on that day. Call data was of no use at this time as it only showed the taxi number on divert calling. Police then applied for call data for the taxi landline number to identify the last number to have contacted Ludlam and any other numbers that might be of interest to the investigation, in order to establish how he might have been lured to the murder scene. The last number to have called the taxi company was attributed to a pre-paid SIM card for which there were no subscriber details. Using the telephone data police were able to identify the place where the telephone had been purchased and where the last top-up before the murder had been purchased, which was at a supermarket petrol station a few days beforehand. The petrol station did not have in-store CCTV but police requested the till records which revealed another transaction of 20 GBP of petrol at the same time as the purchasing of the mobile telephone top-up. Officers now knew the time the top-up was purchased, and so examined all CCTV tapes from locations in the vicinity of the supermarket, which showed a male purchasing a mobile telephone in a nearby shop. This male was identified as Colin Cheetham, who after further investigation was convicted of Ludlam's murder and jailed for 30 years. Without access to relevant traffic data Cheetham might never have been identified.

Case 2

2. A 14-year old female from the Fife area was reported missing in November 2009. She had a history of self-harm and multiple suicide attempts. She had left a note for her parents in which she claimed to have been *"hearing voices"*. A trace to find the live location of the victim's telephone was carried out but it had been switched off. Historical call data was examined to ascertain with whom she had been in contact prior to her going missing. The call data identified a mobile telephone whose subscription was attached to an individual unknown to the girl's parents. Checks at the registered address of the subscriber revealed that the missing girl was in the company of a 36-year-old man whom she had met in an internet chat room. The man was charged with sexual offences.

Case 3

3. UK authorities received intelligence from US authorities that an individual using email had sent a movie file of a woman sexually abusing a four-month-old girl. The log-on IP address for this account was found to be registered to a male from Northampton.

Further enquiries established that a girlfriend of the individual had three children all less than four years old. After investigation both were convicted of the serious sexual abuse of the children. The children had been found in conditions of neglect, described by an officer as filthy, unsanitary and unfit for human residence.

Case 4

4. Internet data were used in an investigation into the grooming of a 13-year-old girl on an internet chat service. Examination of the victim's computer by the authorities revealed the email address of a man who had coerced the girl into sending naked photographs of herself and exposing herself during webcam chat. Police officers made enquiries about the e-mail address which revealed the IP address belonged to an address in Wales. Further investigation resulted in the man being charged preventing potentially more serious sexual offences taking place.

Case 5

5. In 2010/ 2011 police used data from thousands of calls over the previous 12 months between more than a dozen mobile phones to dismantle a nationwide cocaine trafficking ring. Two gang members found to be in possession of 3.58 kg of cocaine (valued 165,000 EUR) were arrested and their mobile phones seized. Detectives then spent months examining communications data to identify links between the other members of the group. This resulted in conviction of six gang members who were sentenced for a total of 53 years imprisonment and the confiscation of 61,000 EUR in cash which is being used to fund police operations targeting other drug dealers.

Case 6

6. Operation Frant was a detailed investigation into a number of drug dealers who were flooding London and the UK with high grade heroin from Afghanistan. The aim was to target the individuals who were masterminding this organised crime network, and as they were not 'hands on' the only possible method of detection was detailed investigation of communications data. The first part of the operation targeted the 'runners' with their consignments. In December 2007 Ghaffor Hussein was arrested in possession of a kilogramme of heroin and in January 2008 Christian Bailey was arrested in possession of 8 kilos of heroin. In April 2008 Harminder Chana and Patrick Kuster (a Dutch national) were arrested in possession of 356 kilos of heroin, having been under surveillance when the exchange took place. One of the ringleaders, Atif Khan, was also arrested later that day on the basis of telephone data and additional surveillance evidence linking him and Chana. Upon arrest all suspects' telephones were seized enabling investigators to obtain the cell site data and establish who orchestrated the deals. Mobile telephone call logs revealed that a certain telephone number had been used to call Khan's telephone 26 times, along with several texts, in a 45-minute period after Khan's arrest. This so-called "*dirty telephone"* was attributed to one Abdul Rob by cell site analysis which showed two mobile phones always in the same place at the same time. The telephone evidence was crucial in the case against Rob as there was no previous surveillance evidence of association with the other members of the network. Four members of the network were convicted for conspiracy to supply heroin and sentenced for total 81.5 years imprisonment.

Case 7

7. In January 2008 customs officers at Birmingham airport discovered over 16 kilos of heroine concealed with straws which had been threaded through rugs imported from Afghanistan, they alerted SOCA. SOCA substituted the drugs rugs with dummies, replaced the original packaging, and began a surveillance operation when the gang came to collect them. After the gang's hire car was abandoned for the second time, SOCA investigators decided to switch from traditional surveillance and to focus instead on their other main lead – a single unregistered mobile telephone number used by the gang to contact the courier company. Analysis of telephone data ultimately led to the identification of five men involved in the plot. All five gang members pleaded guilty on the strength of the telephone evidence. The four main players were sentenced at Birmingham Crown Court in June 2009 to between 10 years 8 months and 14 years 8 months and 14 years 5 months for conspiracy to import Class A drugs.

Case 8

8. Police investigated (Operation Backfill) a series of armed robberies where high value cars were advertised on a website for sale for *"strictly cash only"*. Persons interested in buying the cars went to meet the supposed traders and were robbed at gun point. Police examined internet data and identified the laptop and premises from where the suspects had logged onto the internet when posting the advertisements, leading to a number of arrests.

Case 9

9. In October 2004 a large criminal network conspired to steal £229 million from a bank in the City of London by transferring funds to bank accounts opened in seven different countries. Landline and mobile telephone communication data was critical to establishing those involved in this crime and understanding how it happened. The network members used landline, mobile, and kiosk phones in the UK and across multiple countries. Three defendants were extradited to the UK for trial. Billing data, call data and cell-site location data were all used as evidence in the trial which took place in March 2009. Three defendants were convicted of conspiracy to steal and two were convicted of money laundering.

Annex 11: CRIME TYPES FOR WHICH COMMUNICATIONS DATA IS USED **(7.50(a) above)**

CRIME TYPE	% FOR WHICH COMMUNICATIONS DATA IS USED (OUT OF TOTAL)
Sexual offences	9%
Vulnerable or missing persons	6%
Harassment or stalking	7%
Drugs offences	25%
Homicide, attempted murder & threats to kill	8%
Financial offences	10%
Terrorism	1%
Firearms and explosives	5%
Offences against the person	11%
Offences against property	11%
Other offences	7%

Annex 12: URGENCY OF REQUIREMENTS FOR COMMUNICATIONS DATA **(7.50(b) above)**

The Acquisition Code (footnote 52) explains that the CDSG has adopted a grading scheme to indicate the appropriate timeliness of the response to requirements for disclosure of communications data.

GRADES	% OF USE DURING 2012 SURVEY
Grade 1 – an immediate threat to life	6%
Grade 2 – an exceptionally urgent operational requirement for the prevention or detection of serious crime or a credible and immediate threat to national security	18%
Grade 3 – matters that are routine but, where appropriate, will include specific or time critical issues such as bail dates, court dates, or where persons are in custody or where a specific line of investigation into a serious crime and early disclosure by the CSP will directly assist in the prevention or detection of that crime.	76%

Annex 13: LOCAL AUTHORITY USE OF COMMUNICATIONS DATA

(7.59 above)

1. This annex contains case studies illustrating how councils make use of communications data to stop criminal activity and bring perpetrators to justice.

Operation Magpie – Cambridgeshire County Council

2. Operation Magpie concerned an investigation into an organised crime group who defrauded elderly and vulnerable people. The criminals exploited their victims to the extent that one person was evicted from their home, as well as laundering cheques to the value of £700,000.

3. The ringleader of the gang received a prison sentence of 7 years with two co-conspirators receiving sentences of 5 years each. 16 other offenders were also convicted of money laundering offences serving prison sentences of up to 30 months.

4. Malcolm Taylor from Trading Standards at Cambridgeshire County Council said "*Without access to communications data, we would not have been in a position to connect the conspirators and detect the level of criminality that extended to over 100 vulnerable and elderly victims, some of whom have since died*".

Operation Troy – Suffolk County Council

5. Operation Troy was a long running advanced fee fraud case that was investigated and prosecuted by Suffolk's trading standards service. The fraud operated between 2007 and 2010, involved at least £7.5 million of consumer detriment affecting well over 16,000 consumers and involved two distinct frauds;

6. An escort/companion fraud in which consumers were offered guaranteed work as escorts and companions in return for a registration fee, however no work was subsequently provided.

7. A debt elimination fraud in which consumers paid an advanced fee to receive a debt elimination service but little or no service was ever provided.

8. The fraud was complex and well organised, operating from call centres in Spain. UK customers made contact with the call centres using free phone numbers that appeared to be UK based after viewing various escort websites offering work. During calls with escort agency staff, false promises would be made regarding the immediate availability of work and potential earnings available. Many consumers complained of similar experiences and provided similar accounts of last minute cancelled work appointments after they had paid their fees.

9. The escort websites and telephone numbers changed frequently to confuse consumers and make it difficult for enforcement bodies to track the source of the fraud. By using RIPA powers and obtaining communications data for the telephone numbers used for the fraud, the following links were established:

(a) The multiple telephone numbers were owned and operated by only two individuals. One of those individuals, who held the majority of the numbers, had been identified as being involved in operating multiple UK bank accounts used for money laundering aspects of the fraud and the creation of shell companies.

(b) All the UK free phone numbers were being redirected to Spanish based numbers that were linked to a small number of call centres operating from the Malaga area of Spain. These call centres were all owned by one man who was known to have a previous history of fraudulent trading.

(c) The link provided by this communications data provided evidence that what appeared outwardly to be over 12 different separate escort website/agencies were in fact all one fraud perpetrated by one set of linked individuals.

10. In June 2012 European Arrests warrants were applied for in respect of Antoni Muldoon, the man at the helm of the fraud, and two other members of the gang, Geraldine French and Bradley Rogers. All three were returned to the UK. Following extradition in September 2012 Muldoon pleaded guilty to conspiracy to defraud at Ipswich Crown Court.

11. Following Muldoon's plea, and after a series of trials at Ipswich Crown Court including a ten week trial involving five of the defendants that concluded in June 2013, seven further members of the gang were found guilty of offences including conspiracy to defraud and money laundering offences. The sentences handed down totalled 36 years overall, with Muldoon receiving 7.5 years for his role and Mark Bell of Ipswich, Muldoon's right hand man in the UK, receiving 6.5 years.

12. Confiscation proceedings followed the sentencing and to date £315,000 has been awarded in confiscation and costs, which Suffolk Trading Standards has used to repay victims of the fraud. Confiscation proceedings are continuing against Antoni Muldoon who is known to have benefited to the largest extent from this fraud and the amount of confiscation possible from him is expected to be substantial. Confiscation hearings for Muldoon are set to take place in January 2015.

13. In July 2014 four of the defendants appealed their convictions and sentences at the Court of Appeal in London and in front of three sitting High Court Judges all appeals were turned down.

14. Steve Greenfield, Suffolk's Head of Trading Standards and Community Safety commented that "*RIPA powers were essential to the successful outcome of this case*".

Counterfeit goods case study 1

15. Two internet traders based in Slough were selling counterfeit trainers on e-bay for £35.00. The only intelligence the trading standards service had was the e-mail address and mobile phone numbers that the complainants used to make the purchase. The actual retail price of these trainers was £135 a pair. By obtaining the data from the mobile phones and the IP address the council were able to pinpoint the address being

used by the perpetrators. A test purchase had been made prior to a warrant being sought. A sting operation resulted in a seizure of trainers with a street value of £325,000 and both offenders received a custodial sentence. Without the communications data this would not have been possible.

Counterfeit goods case study 2

16. Officers seized some potentially counterfeit mirrors from a shop. By the time the mirrors were confirmed as being counterfeit the trader had disappeared after failing to attend for interview. The contact details he provided proved to be false. However, officers obtained a mobile number for the trader and the subscriber details identified his home address in Swansea. This enabled officers to contact him. He subsequently pleaded guilty to 3 offences under the Trade Marks Act 1994. Without the access to the communications data officers would not have been able to find the new address to which he had moved and so the investigation would not have been able to proceed.

Barnet council – rent deposit scheme fraud

17. A man and woman were jailed following a Barnet Council investigation to crack a highly organised plot to obtain fraudulent payments from the authority by using a complex web of false identities to open a string of bank accounts which were then activated to receive thousands of pounds in fraudulent rent deposit scheme payments. The rent deposit scheme is used by the council to provide people in need of housing with initial financial support to help secure a tenancy for private rented accommodation.

18. The investigation by the council's Corporate Anti-Fraud Team **[CAFT]** was launched after uncovering irregularities with a number of rent deposit payments. Investigators went on to identify 41 fraudulent payments worth £132,629 which had been paid to different bank accounts. During the course of the investigation a further 12 fraudulent payments worth more than £31,600 were intercepted and blocked by CAFT.

19. CAFT worked with NAFN to obtain mobile phone records, under RIPA, which provided significant evidence to show that the accused were in regular contact on the days when substantial withdrawals and deposits were made. The powers also enabled the investigators to identify the real owners of the false identities by obtaining the mobile phone service providers records which identified names and addresses where these suspects could be found. The legislation also allowed information of redirected post from credit card companies, banks and online purchase deliveries which also assisted in tracing addresses that the suspects used which were then the subjects of police / CAFT raids. Without access to this information the investigation would not have proceeded to a useful outcome.

Landfill tax fraud

20. A council was alerted to a skip hire company who were disposing of waste in an unauthorised manner, including avoiding payment of landfill tax estimated at £1.3 million. Enquiries made by the council identified three suspects but there was no evidence to link them to the offences. Subscriber and itemised billing data provided by NAFN proved that there were regular communications between the individuals

during periods in question. Without this information, it would have been impossible to pursue a prosecution.

Fraudulent car trader

21. A car trader was convicted of multiple offences contrary to the Fraud Act 2006 in relation to the sale of misdescribed and clocked cars. Vehicles were purchased at auction with higher mileage and advertised online via AutoTrader. The trader claimed a third party was responsible and he simply allowed the third party to use his account at auction to obtain vehicles more easily. However, SIM cards found in possession of the car trader were confirmed, using communications data, as being associated with unregistered pay as you go telephone numbers used in adverts for vehicles. During the course of the investigation, the trader sold his house and moved location; a second set of communications data (forwarding address details from Royal Mail helped to locate him for the purposes of arrest, entry warrants and interview. The penalty was 12 months imprisonment and a Proceeds of Crime Act 2002 confiscation order in excess of £58,000.

Annex 14: LOCAL AUTHORITY RIPA COMMUNICATIONS DATA REQUESTS VIA NAFN (9.100 above)

	2012	2013	2014	2015
January	247	190	81	158
February	328	204	106	190
March	341	313	146	
April	270	230	78	
May	383	136	83	
June	233	208	71	
July	292	335	1563[19]	
August	338	246	166	
September	292	129	110	
October	496	337	119	
November	150	201	62	
December	198	175	91	
Total	**3568**	**2704**	**2676**	

[19] The July 2014 one-off surge involved a criminal investigation by one local authority in relation to a suspected £multi-million conspiracy to defraud. The application included approximately 1300 requests for subscriber checks and itemised billing.

Annex 15: THE LAW OF THE FIVE EYES (8.41 above)

Australia

1. The primary statute governing access to intercept and communications data in Australia is the TIA 1979.[20] It is long and complex.

2. It distinguishes between "*interception*" of communications that are passing through a telecommunications system and "*access*" to stored communications on a carrier's equipment, although both are only lawful when carried out pursuant to a warrant. Interception is narrowly confined to "*real time*" communications: "*listening to or recording by any means, such a communication in its passage … without the knowledge of the person making the communication*."[21] Once a communication has become accessible to the recipient, it is no longer passing over a telecommunications system and must be accessed via a stored communications warrant.[22]

Interception

Australian Security Intelligence Organisation

3. The TIA 1979 Part 2-2 sets out the mechanism by which ASIO (the Australian equivalent of MI5, governed by the Australian Security Intelligence Organisation Act 1979) might be issued with a warrant to intercept communications. ASIO cooperates with the Australian Secret Intelligence Service **[ASIS]**, the Australian Signals Directorate and the Australian Geospatial-Intelligence Organisation.

4. ASIO may apply for, three types of warrant to intercept communications in order to access the communications of a person who is reasonably suspected of being engaged in or likely to engage in activities prejudicial to security.[23] Each of those warrants may be issued by the Attorney-General on request by the Director-General of Security:

   (a) A warrant that specifies the telecommunications service likely to be used by a person engaged in activities prejudicial to security;[24]

   (b) A named person warrant that grants authority to intercept the various communications methods employed by an individual (all their mobile phone numbers or email addresses);[25]

   (c) A B-party warrant, which enables the interception of a service that will be used by a non-suspect to communicate with a suspect.[26]

---

20 The Surveillances Devices Act 2004 and the Telecommunications Act 1997 contain further relevant provisions.
21 TIA 1979 s6(1).
22 TIA 1979 s5F(1). If only the telecommunications data is required, then stored material may be accessed without a warrant under s 178 and 179 of TIA.
23 TIA 1979 s9(1).
24 TIA 1979 s9(1).
25 TIA 1979 s9A.
26 TIA 1979 s9(1)(a)(ia).

5. Accordingly, national security warrants may only be obtained for quite narrow purposes; they do not provide a basis for bulk interception. Section 10 sets out a mechanism for the issuing of emergency warrants, when the Director General of Security considers it appropriate, for no longer than 48 hours.

6. A separate regime governs the grant of warrants where ASIO wishes to intercept "*foreign intelligence"*. In each case, the Attorney-General must be satisfied, on the basis of advice from the Minister of Defence or Foreign Affairs, that obtaining the foreign intelligence set out in the notice is in the interests of Australia's national security, foreign relations or economic well-being. Once again, three types of warrant may be issued:

   (a) A warrant authorising interception on quite a general level to a particular "*telecommunications service*." Where known, the name and address, occupation and number of the subscriber should be set out in the request.[27]

   (b) A named person warrant, for which the application must specify the telecommunications service that is being used by a person or foreign organisation and the foreign intelligence information that will be obtained.[28]

   (c) A "*foreign communications*" warrant for the interception of foreign communications only, (those sent or received outside of Australia.[29]

7. The Director-General must not request the issue of a foreign intelligence warrant under s 11A, 11B or 11C for the purpose of collecting information concerning an Australian citizen or permanent resident.[30]

Law Enforcement Authorities

8. The TIA 1979 Part 2-5 sets out the circumstances in which law enforcement bodies may intercept telecommunications. They may apply for a warrant to an eligible Judge or a nominated member of the Administrative Appeals Tribunal **[AAT]**. A range of agencies can apply, at both the state and federal level, including the Independent Broad-based Anti-Corruption Commission and various Crime Commissions.[31]

9. The application must be supported by an affidavit setting out the facts and other grounds on which it is based. Two types of warrant may be issued:

   (a) A telecommunications service warrant, which authorises the interception of a particular telecommunications service that may be used by an identified individual. It must set out the number of previous applications (if any) related to the service or that person and the use made by the agency of information obtained by interceptions under those warrants.

27 TIA 1979 s11A(1).
28 TIA 1979 s11B.
29 TIA 1979 s11C.
30 TIA 1979 s11D(5).
31 TIA 1979 s39.

(b) A named person warrant, which must set out the name of the person and details sufficient to identify the telecommunications service they are using, details of previous applications and use made of the material obtained.[32]

10. The Judge or AAT member must be satisfied that there are reasonable grounds for suspecting that a particular person is using or is likely to use the service and the information that would be likely to be obtained would be likely to assist in connection with the investigation by the agency of a serious offence.

11. The Judge or AAT member should have regard to:

(a) How much the privacy of any person or persons would be interfered with;

(b) The gravity of the conduct constituting the offence;

(c) The value of the information obtained;

(d) The extent to which other methods have been used, would be likely to assist, or might prejudice the investigation.

12. They must be satisfied that all other practicable methods of accessing the communications have been exhausted.[33]

13. Warrants may be sought and obtained, in urgent circumstances, via telephone.[34]

Stored Communications

14. The TIA 1979 Part 3 contains a separate regime governing access to stored communications. In broad terms, both ASIO and criminal law enforcement agencies are entitled to issue preservation notices, requiring a carrier to preserve all stored communications specified in the notice.[35] The notice may only specify one person or telecommunications service.[36] The TIA 1979 distinguishes between a domestic preservation notice and a foreign preservation notice. A foreign preservation notice is issued when a foreign country intends to request the Attorney-General to secure access to telecommunications. In that sense, they reflect the UK's MLAT regime.[37]

15. ASIO does not have to apply for a preservation notice before seeking access to material on the basis of a warrant. It may apply for a warrant in any case where it reasonable grounds for suspecting that a particular carrier holds stored communications that is likely to assist in connection with the investigation of a serious contravention (a crime of sufficient seriousness).[38] Furthermore, ASIO does not normally have to apply for a separate stored communications warrant. An interception warrant will also entitle them

32 TIA 1979 ss42 and 46A.
33 TIA 1979 ss46 and 46A.
34 TIA 1979 ss43 and 50.
35 Recent changes have added a new TIA 1979 s110A that has restricted the power to access stored telecommunications data to "*criminal law enforcement agencies*", rather than the broader law enforcement agencies described above.
36 TIA 1979 s107H(3).
37 TIA 1979 s107N.
38 TIA 1979 s106(c).

to access stored communications if the warrant would have authorised interception if it were still in passage.[39] However, a criminal law enforcement agency will need to apply for a stored communications warrant.

16. TIA 1979 contains a number of provisions relating to the destruction of material obtained via warrants.

Telecommunications data

17. TIA 1979 Part 4 sets out the circumstances in which bodies may obtain access to telecommunications data. Telecommunications data is not formally defined, although it does not include the contents or substance of a communication.[40] A new mandatory data retention regime specifies categories of information that must be kept by service providers for a period of two years.[41] These categories include the subscriber of a relevant service and the source, time, date, and location of a communication.[42]

18. Sections 174-6 provide for three types of disclosure of telecommunications data to ASIO. Firstly, on a voluntary basis by a service provider "*if the disclosure is in connection with the performance by* [ASIO] *of its functions*." Secondly, an authorisation for access to existing information or documents (which may be granted by the Director General of Security, Deputy Director General of Security and an officer of ASIO approved by the Director General). Thirdly, a slightly wider body of individuals may authorise access to prospective information (anybody above a certain level of seniority within ASIO may grant permission), for not longer than 90 days.[43] In the case of an authorised disclosure, the authorising individual must be satisfied that the disclosure would be "*in connection with the performance by* [ASIO] *of its functions*".

19. Sections 177-180 set out the framework governing the disclosure of existing telecommunications data to enforcement agencies (which includes any criminal law enforcement agency). An enforcement agency may authorise the disclosure of telecommunications data where reasonably necessary to enforce the criminal law, locate missing persons, enforce a law imposing a pecuniary penalty or protect the public revenue. Accordingly, bodies that have the power to levy a fine may seek access to telecommunications data.[44] The disclosure of prospective telecommunications data may be authorised for a limited period where reasonably necessary for the investigation of a serious offence.[45]

20. Sections 180A and 180E allow authorised officers of the Australian Federal Police to obtain access to telecommunications data for the purpose of further disclosing that material to a foreign authority. The procedure, as with intercepted material, is similar to the UK's MLAT process.

---

39 TIA 1979 s109.
40 TIA 1979 s172.
41 TIA 1979 s187C.
42 TIA 1979 s187A.
43 TIA 1979 ss175-6.
44 As long as they are defined as an enforcement agency in the newly amended TIA (see s110A).
45 TIA 1979 s180.

21. Before any authorisation is made (on any of the bases set out above) the authorised officer considering making the authorisation must be satisfied on reasonable grounds that any interference with privacy is justifiable and proportionate.[46]

22. An authorisation, the notification of that authorisation, revocation and notification of the revocation must be in written or electronic form, and must contain:

    (a) The identity of the eligible person and the basis on which they are eligible to make the authorisation;

    (b) The person or company from whom the disclosure is sought;

    (c) Details of the information or documents to be disclosed;

    (d) A statement that the eligible person considers that to be in connection with ASIO's functions; and

    (e) The date of the authorisation. [47]

23. Authorisations made on behalf of an enforcement agency must set out certain additional material. The rules are very detailed and vary, depending on whether the material is historic or prospective and on behalf of a foreign government or not.

24. Each year, the head of an enforcement agency must give the Minister a written report that sets out the number of authorisations made and the number of disclosures to foreign countries and names of those countries. The minister consolidates that material and lays before Parliament a report that sets out the consolidated material.[48]

The Australian Secret Intelligence Service

25. Different provisions apply to the activities of ASIS (the equivalent of MI6), which are controlled by the Intelligence Services Act 2001 **[ISA 2001]**.

26. ASIS may gather intelligence about an Australian person or class of Australian persons outside Australia, as long as this is authorised by the Minister for Foreign Affairs.[49] The Minister must be satisfied that gathering the intelligence is necessary for the proper performance of one of ASIS's statutory functions, and the person or class of persons is involved in one of a list of specified activities (such as acting for a foreign power, or other activities that pose a threat to Australia's security).[50] ISA 2001 s14 waives any liability for ASIS in respect of acts committed overseas that would be unlawful if done pursuant to a proper function of the agency. That waiver does not extend to activities inside Australia that ASIO could not carry out without a warrant, but it may well include interceptions overseas.

---

46 TIA 1979 s180F.

47 The Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2012, drafted by the Communications Access Co-ordinator.

48 TIA 1979 s186.

49 TIA 1979 s9.

50 ISA 2001 s9.

Oversight

27. Oversight of the interception process is provided in Australia by three mechanisms. Firstly, the Parliamentary Joint Committee on Intelligence and Security oversees the administration and expenditure of the Australian intelligence community, including ASIO. It is made up of members of both houses of Parliament nominated by the governing party, in consultation with all the parties in Parliament, although with a majority made up of the party currently in government. It reports to Parliament once a year, and will also review any amendments to include new agencies in the list of those which may authorise the disclosure of metadata.[51]

28. Secondly, the Inspector General of Intelligence and Security **[IGIS]** is established by the Inspector General of Intelligence and Security Act 1986 **[IGIS Act]**. It is a largely investigatory role, appointed for five years. He carries out broad-ranging investigations into the actions of the agencies at his own initiative or pursuant to a complaint or a request from the public or from ministers, including the Prime Minister.[52] He must seek the approval of the Prime Minister or a responsible Minister before investigating actions that took place outside of Australia.[53]

29. The IGIS is appointed by the Governor-General on the advice of the Prime Minister. The office is accountable to the Prime Minister but does not take directions from him. IGIS provides an annual report to the Prime Minister, who may redact that report before laying it before Parliament, although an unredacted version must be made available to the leader of the opposition.

30. As part of his role, IGIS also conducts regular inspections and investigations. Amongst those inspections are regular reviews of the documents that ASIO has relied on as providing the basis for its interception warrants.

31. Thirdly, the Commonwealth Ombudsman investigates the use of interception powers by law enforcement agencies, including through regular inspections of their records.[54] The office does not have jurisdiction over the intelligence agencies.[55] The Ombudsman must also inspect the records of enforcement agencies to determine their compliance with the new metadata regime.[56]

Canada

32. Canadian law provides a separate authorisation mechanism for the police and the security services to collect data.

Criminal law enforcement

33. Part VI of the Criminal Code, added pursuant to the Protection of Privacy Act 1974, provides for the grant of judicial warrants to intercept private communications. Private

---

51 TIS 1979 ss110A(11) and 176A(11).
52 IGIS Act s8.
53 IGIS Act s9AA.
54 Ombudsman Act 1976 s5.
55 Ombudsman Regulations 1977 sch. 1.
56 TIA 1979 s186B.

communications are defined as "*any oral communication or any telecommunication that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator thereof to expect that it will not be intercepted by any person other than the person intended by the originator thereof to receive it.*"

34. In order to obtain an interception warrant, the police must make an application to a judge of a superior court of criminal jurisdiction that is signed by the Attorney General of the province in which it is made (or an agent specified for this purpose by the Government). It must be accompanied by an affidavit setting out (s185):

> "... (c) the facts relied on to justify the belief that an authorization should be given together with particulars of the offence;
>
> (d) the type of private communication proposed to be intercepted;
>
> (e) the names, addresses and occupations, if known, of all persons, the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence, a general description of the nature and location of the place, if known, at which private communications are proposed to be intercepted and a general description of the manner of interception proposed to be used;
>
> (f) the number of instances, if any, on which an application has been made under this section in relation to the offence and a person named in the affidavit pursuant to paragraph (e) and on which the application was withdrawn or no authorization was given, the date on which each application was made and the name of the judge to whom each application was made;
>
> (g) the period for which the authorization is requested; and
>
> (h) whether other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures."[57]

35. The application is made *ex parte* and is heard confidentially. However, targets of interceptions must be given notice of that fact they have been subject to surveillance, within 90 days of the authorisation having expired. A confidentiality extension may be granted up to three years after the investigation has come to a close (s196) in terrorism offence cases, where the judge is persuaded that it is in the "*interests of justice*". There are special provisions for obtaining an urgent authorisation from the judge (s188).

36. Stored communications, for example in cloud storage or on a personal computer, may also be accessed via a production order or search warrant. A search warrant may be granted by a judge who is satisfied that there are reasonable grounds to believe that there is "*anything on or in respect of which any offence"* has been or is suspected to

[57] Subsection (h) does not apply to some serious crimes and terrorism offences.

be committed, or evidence as to commission of an offence or the whereabouts of a person who is believed to have committed an offence.[58] A judge may also order a person, other than a person under investigation for an offence, to produce documents or prepare a document based on data already in existence and produce it.[59]

37. There is some confusion within Canadian law concerning whether emails that have already been sent should be governed by intercept or search warrants. In *R v Telus* (2013) SCC 16, the Supreme Court interpreted "*interception*" purposively, holding held that a warrant requiring a service provider to prospectively provide access to text messages was invalid: the police were seeking an "*interception*," as the service provider stored text messages on their servers as part of the communication and transmission process. Thus it is likely that the Royal Canadian Mounted Police should use their intercept powers, not those for search warrants, when seeking prospective access to email.

38. In late 2014, the Canadian Parliament passed the PCFOC 2014 that amended certain aspects of the Criminal Code. It provided for a clearer and more comprehensive framework for access to metadata by judicial warrant or court order, on a "*reasonable grounds to suspect*" standard (one that is lower than the more traditional reasonable grounds to believe threshold).[60]

Access for the Security Services

39. The CSIS are regulated by the CSIS Act 1984, which distinguishes between "*security intelligence*" and "*foreign intelligence."* The former relates to national security threats; the latter to the political or economic activities of foreign states. Save in relation to the s16 exception set out below, CSIS's role relates to the collection and analysis of security intelligence, and it is broadly the equivalent of MI5.

40. The CSIS Act 1984 s12 provides, where relevant:

> "The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada."

41. The s16 exception provides that the service may collect information or intelligence in relation to any foreign state as long as that information does not relate to a Canadian citizen, permanent resident or Canadian corporation and is done in Canada.

42. Warrant applications are made to a special bank of 14 specially selected and security cleared Federal Court judges, who meet up twice a year to ensure consistency. They largely hear warrant applications alone but may sit in larger numbers to hear an application and to hear submissions from CSIS on a topic of wider interest, although in

---

58 Section 487.1.

59 Section 487.12. A separate provision concerns provision of financial data of those suspected of Terrorist Financing or Money Laundering (487.13).

60 Criminal Code 417.014-018.

such cases the substantive decision is still taken by a single presiding judge. They are entitled to appoint an *amicus* advocate to make submissions in respect of the privacy issues raised by the application. I was told, in the course of my meeting with several judges of the Court, that they frequently appoint *amicus* counsel when novel warrants are sought that deploy new technology or propose new applications of old technology. The members of the Court were of the view that those counsel provided them with real assistance. I was told that warrant applicants can be made, heard and determined within 24 hours, and dealt with even faster in an emergency. The ordinary time lag is around 3 days.

43. The applicants are subject to a high duty of candour and may not omit relevant or important information. They will be criticised for failing to do so, as they were in *X(Re)* (2013) FC 1275, when Judge Mosley concluded they had deliberately suppressed their intention to monitor Canadian terror suspects outside of Canada (via cooperation with other Five Eyes members).[61]

44. In addition to the judges (who sit on rotation), the Designated Proceedings Registry employs eight full time staff and one full time senior counsel. The Registry's annual budget (excluding infrastructure and some IT costs) was $826,000 last year (*circa* £430,000). During 2013-14 the Federal Court dealt with 85 new warrant applications and 178 renewal applications.

45. A warrant must be supported by an affidavit, which I am told are ordinarily between 35 and 200 pages long. They set out (amongst other things):

    (a) Why the applicant believes "*on reasonable grounds*" that the warrant is necessary for the Service to carry out its role;

    (b) Other procedures have been tried and failed or are unlikely to succeed;

    (c) The type of communication to be intercepted or information, records, documents or things to be obtained;

    (d) The identity of the person whose communication is proposed to be intercepted (if known); and

    (e) Any previous applications in respect of that person.

46. A warrant may not be issued for longer than 60 days, where it is issued to enable the Service to investigate "*threats to the security of Canada*", or one year in any other case.

47. Thus, this warrant process involves a two-stage review process: by the Minister and also by the court. The judicial element was introduced following a series of reports into abuses carried out by the Canadian police Security Services in the 1970s.

48. In 2008 in *Re CSIS*, the Federal Court held that the CSIS had no power to carry out activities beyond Canadian borders because the CSIS Act is not extraterritorial in scope, or at least did not authorize overseas conduct that was not in compliance with

[61] The judgment was upheld by the Court of Appeal (*Re(X)* 2014 FCA 249)

foreign laws (and thus violated foreign sovereignty). As a practical result, the power to covertly collect information (pursuant to a s21 warrant) relating to foreign affairs is restricted to the right to take steps within Canada itself. The effects of that decision were reversed by PCFOC 2014 which provided that CSIS may perform its duties and functions outside of Canada. It expressly authorises a judge to issue a warrant for overseas investigations, even if those investigations may be violation of foreign or other laws.

49. Sections 34 and onwards of the Act establish the SIRC, composed of members of the Canadian Privy Council. Those who sit on SIRC are not ordinarily members of the Senate or House of Commons. The Governor in Council (in practice, the Canadian federal cabinet) appoints the members of the Committee in consultation with the Prime Minister, Leader of the Opposition and the leader of each party with at least 12 Members of the House of Commons. The individuals appointed play an important but comparatively limited role in the operations of SIRC. They retain other obligations and ordinarily only meet a small number of times per year. The day-to-day operations of SIRC are carried out by its full time staff of 18 individuals.

50. The Committee is required to review the Service in general, although the statute does not specify that it should review the warrantry process. However, in practice SIRC reviews a random sample of all warrant applications in any given year (around 5%). That review involves an examination of the underlying documents that led to the warrant application, that were not provided to the court in the application. Their reports are provided to the Minister and the Director of the Service. SIRC also prepares an annual report recounting its operations and summarising its findings and recommendations.

51. Any individual may complain of the Service's activities to the Committee, which is entitled to investigate and make recommendations. .[62] SIRC has no powers to enforce its holdings. It is competent only to make recommendations.

52. The National Defence Act 1985 **[NDA 1985]** recognised the existence of what is now the CSE, a signals intelligence agency and the Canadian equivalent of GCHQ. NDA 1985 defined CSE's mandate as:

> "(a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
>
> (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
>
> (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties."[63]

62 Section 37.
63 273.64(1).

53. In conducting its mandate (a) and (b) functions, CSE may not direct its activities at Canadians or any person in Canada and their activities are subject to measures to protect the privacy of Canadians in the use and retention of intercepted material. When CSE performs its mandate (c) function providing assistance to federal law enforcement and security services, it is sheltered by those bodies' lawful authority (e.g., a Part VI authorization or CSIS Act warrant).

54. When CSE collects foreign intelligence, this is generally an internal decision with no legislated oversight requirements. However, in the course of collecting foreign intelligence through signals intelligence operations, CSE may sweep up incidental "*private communications*" – that is communications involving Canadians or persons in Canada. To prevent this from being a violation of the Criminal Code's Part VI prohibition on unlawful intercepts, the NDA 1985 puts in place a special authorization regime, involving the Minister of National Defence. Unlike CSIS, CSE may be authorised by the Minister to obtain foreign intelligence that may involve private communications without reference to the courts. The Minister must be satisfied that the interception will be directed at foreign entities outside Canada, the information could not be obtained by other means, the value of the material justifies the interception and that satisfactory measures are in place to protect the privacy of Canadians and to ensure that the material will only be used or retained if they are essential to international affairs, defence or security. These broad powers stand in some contrast to the focused and specific warrantry process for CSIS.

55. While CSE has historically adopted the position that a ministerial authorisation was not required before it obtained access to metadata, following *Telus* and *Spencer*, and the changes introduced by PCFOC 2014, that position is no longer arguable.

56. NDA 1985 requires the appointment of a supernumerary (retired) judge as a Commissioner of CSE to review its activities and investigate any complaints (section 273.63). The current Commissioner is supported by 11 staff members. His operation costs a little under $2 million Canadian dollars per year.[64] Among other things, the Commissioner reviews any new ministerial authorisations relating to private communication on a provisional basis and then addresses them in more detail in his annual review. His staff are also given access to the data analysis engineers within CSE and may confirm the processes and uses that it is subjected to.

57. The Commissioner's reports have been an important source of information concerning what mechanisms are employed by CSE and also how it interprets its obligations. In particular, the 2012 Commissioner's report disclosed CSE's policy concerning the private communications of Canadian citizens that are the 'bycatch' of a foreign intelligence collection:

    (a) They must be destroyed, save where the material is foreign intelligence or material essential to protect the lives or safety of individuals of any nationality, or where it contains information on serious criminal activity relating to the

64 http://www.ocsec-bccst.gc.ca/ann-rpt/2013-2014/ann-rpt_e.pdf p. 13.

security of Canada or is essential to identify, isolate or prevent harm to the Canadian Government's computer systems.

(b) At the expiry of an authorisation, CSE must report to the Ministry of National Defence explaining what Canadian communications were retained and on what basis.[65]

(c) When CSE shares information with its global partners, the names of any Canadian are redacted and only reinstated at the specific request of a partner country and after CSE has satisfied itself that the requesting government department has proper authority and justification to make the request.[66]

New Zealand

The Security and Intelligence Service

58. NZSIS is New Zealand's equivalent of MI5, and is governed by the New Zealand Security Intelligence Service Act 1969 **[SISA 1979]**.

59. Like Canada, America (and to some extent Australia), New Zealand provides for judicial oversight of the warrant process at the point of authorisation. However, unlike those countries, that oversight is provided by a retired High Court Judge, the Commissioner of Security Warrants. The Commissioner is a creature of statute, created in 1999.[67]

60. Domestic warrant applications are jointly signed off by both the Minister and the Commissioner. The applicant must provide sworn witness evidence that the interception is necessary for the detection of activities prejudicial to security or for the purpose of gathering foreign intelligence information essential to security. They must also provide evidence that any communication sought to be intercepted is not privileged and that the information is not be obtained by any other means.[68]

61. Foreign intelligence warrants operate differently. Firstly, the Commissioner is not involved in their authorisation. Secondly, as well as satisfying the conditions above, NZSIS must demonstrate that that there are reasonable grounds for believing that no New Zealand citizen or permanent resident is to be identified by the proposed warrant as a person who is to be subject to the warrant and that any place to be specified in the proposed warrant is occupied by a foreign organisation or a foreign person.

62. Whether internal or foreign, intelligence warrants must specify the type of communication to be intercepted, the identity of the persons (if known) whose communications are sought to be intercepted and (if not known) the place or facility in respect of which communications may be intercepted.[69] Given the restrictive nature of those requirements, it is unlikely that NZSIS has any power to carry out bulk interception.

---

65 *Ibid.,* p. 14-15.
66 *Ibid*., p. 27.
67 SISA 1979 s5A.
68 SISA 1979 s4A.
69 SISA 1979 s4B.

63. SISA 1979 also contains provisions relating to destruction of irrelevant data.

The Government Communications Security Bureau

64. The GCSB was originally a branch of the Ministry of Defence. It bears some resemblance to GCHQ in the United Kingdom. The Director of GCSB may apply in writing to the Minister for an interception warrant authorising the interception of:[70]

(a) Communications made or received by one or more persons or classes of persons specified in the authorisation or made and received in one or more places or classes of places specified in the authorisation;

(b) Communications sent from, or being sent to an overseas country; or

(c) The accessing of one of more specified information infrastructures or classes of information infrastructures that the Bureau cannot otherwise lawfully access.

65. As under SISA 1979, any application for a warrant or access authorisation must be made jointly to the Minister and the Commissioner of Security Warrants, if anything done under the warrant is for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident.[71] If the warrant or authorisation is not sought for the purpose of intercepting the private communications of a person who is a New Zealand citizen or permanent resident, only the Minister needs to agree it.[72]

66. The Minister and Commissioner may grant the interception warrant if satisfied that it is for the purpose of performing the Bureau's functions; the outcome justifies the interception; it cannot be achieved by other means; there are satisfactory arrangements to ensure that nothing will be done in reliance on the warrant that goes beyond what is necessary; and anything done will be reasonable, having regard to the purposes of the warrant itself.[73] As with SISA 1979, no warrant may be issued for the purpose of intercepting privileged communications.

67. Interception without a warrant may take place in certain narrow circumstances, when the interception does not involve physically connecting an interception device to any information infrastructure or installing an interception device in a place; any access to information infrastructure is "*limited to access to one or more communication links between computers or to remote terminals*" and it is carried out in pursuance of either advising or cooperating with public authorities in terms of protecting communications and infrastructures, or regarding foreign intelligence.[74]

Police Surveillance

68. The Search and Surveillance Act 2012 **[SSA 2012]** sets out a comprehensive regime governing all species of warrant, including warrants for entry, warrants to set up road blocks and interception under a warrant. A warrant is necessary if an enforcement

70 GCSB Act s15A(1).
71 GCSB Act s15B.
72 GCSB Act s14.
73 GCSB Act ss15A(2).
74 GCSB Act s16.

officer wishes to use an interception device to intercept a private communication (as well as various other forms of surveillance).[75]

69. An application for a surveillance device warrant (which includes a warrant to use an interception device) must be made in writing and set out in "*reasonable detail*": the name of the applicant, the provision that authorises the application, the grounds on which it is made, the suspected offence in relation to which authorisation is sought, the type of device, the name address or other description of the person, place, vehicle or thing that is the object of surveillance, what material it is hoped to obtain and the period for which the warrant is sought.[76] If the person, place, thing or vehicle cannot be identified, the application must at least define the parameters of and objectives of the operation. An application may only be made by a constable or an enforcement officer that has been approved by an Order in Council.[77]

70. Other law enforcement bodies than the police may only undertake interception if they have been designated by an Order in Council made by the Governor-General.[78]

71. The application should be made to a Judge, who must be satisfied that there are reasonable grounds to suspect that an offence has been or is being or will be committed and that that offence falls within a list of sufficiently serious crimes, set out in the Schedule to the Act.[79] The Judge must also be convinced that the interception will obtain evidential material.

72. There are mechanisms for obtaining a warrant in an emergency, where there is insufficient time to secure access to a Judge.[80]

Access to Metadata

73. The law concerning access to communications data, or metadata, was unclear until recently. In 2013 it was disclosed that GCSB had taken the view that metadata was not a communication and so could be obtained without a warrant (or indeed any other formal authorisation mechanism).[81] TICSA 2013 has set the position out on a statutory footing. It defines "*call associated data*" as information generated as a result of making a telecommunication that includes the number from which it originates, the number to which it was sent, if it is diverted then the number at which it was received, the time at which it was sent, its duration, if it was from a mobile phone the point at which it first entered the network.[82]

74. Public telecommunications service providers are required to be capable of obtaining call associated data (other than telecommunications that are not authorised to be intercepted under the warrant or lawful authority).[83] That information should be

75 SSA 2012 s46.
76 SSA 2012 s49(1).
77 SSA 2012 s49(5).
78 SSA 2012 s50(1).
79 SSA 2012 s51(1).
80 SSA s48.
81 Kitteridge Report on GCSB Compliance, available online at: http://www.gcsb.govt.nz/assets/GCSB-Compliance-Review/Review-of-Compliance.pdf para 23.
82 TICSA 2013 s3.
83 TICSA 2013 s10.

provided, on presentation of a proper warrant, to GCSB, SIS or the New Zealand Police.

75. A fresh round of Snowden disclosures in 2014 suggested that GCSB had developed a mass metadata collection program known as SPEARGUN. The basic premise of the alleged program was to insert metadata probes into the Southern Cross Cable, which carries much of New Zealand's telecommunications. Prime Minister John Key admitted that the project had been initiated but denied that it had become operational because he had vetoed it. The controversy arose, in part, as the broad powers under GCSB Act ss15 and 15A were not in place during 2012, when the project was allegedly begun.[84]

Oversight

76. The New Zealand security services are overseen via a number of statutory mechanisms. First, the Intelligence and Security Committee is a Parliamentary body, established in statute, which is made up of five persons including the Prime Minister, Leader of the Opposition and 3 other Members of Parliament.[85] It examines the policies and administration of the Security Intelligence Service and GCSB and consider other questions with intelligence or security implications that are referred to it by the Prime Minister.

77. Second, the Inspector-General of Intelligence and Security, is an individual appointed by the Governor General, on the recommendation of the Prime Minister.[86] The Inspector-General enquires into the Services' compliance with its legal obligations and complaints about its activities. They are specifically required to review, at least once every 12 months, the compliance with the governing legislation in relation to the issue and execution of warrants and authorisations.[87] The Inspector-General reports annually to the Prime Minister and a redacted version of that report is laid before Parliament.

78. Third, as set out above, the Commissioner of Security Warrants is engaged in agreeing to any warrant granted to the security service that will collect the communications of New Zealand citizens or residents.

The United States of America

79. The US law concerning investigatory powers is divided between two separate statutory frameworks. The WA 1968, the Stored Communications Act **[SCA]** and Pen Register Act **[PRA]** govern the use of investigatory powers in conventional criminal law enforcement.[88] A separate regime, the Foreign Intelligence Services Act 1978 **[FISA 1978]**, governs the collection and analysis of foreign intelligence. Both frameworks have been extensively amended since their introduction.

---

84 https://firstlook.org/theintercept/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance/
85 Intelligence and Security Committee Act 1996.
86 Inspector-General of Intelligence and Security Act 1996 **[IGISA]** s. 5.
87 IGISA s11(d).
88 US Civil Code Title 18 Chapter 119. SCA and PRA were introduced under the Electronic Communications Privacy Act 1986, which substantially amended the WA 1968.

Criminal law enforcement

80. The WA 1968 governs interception of wireless, oral and electronic communications within the United States. It defines intercept as "*the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.*"[89] Access to information that is not in the course of transmission, is governed by the SCA.[90]

81. All interceptions under the WA 1968 must be authorised by a court and are subject to careful review. US Code s2516 of Title 18 sets out the basis on which law enforcement staff, inside the United States, may be given authority to intercept communications. Various senior officials within federal law enforcement agencies (such as the FBI or the Attorney General's office) may authorise an application to a Federal Judge of competent jurisdiction for an interception warrant.[91] The application must be in writing, on oath and set out the facts and circumstances in some detail. I was told by law enforcement agencies that these applications are frequently substantial documents. An application may only be made in order to provide evidence (from the wiretap) that will be relevant to certain serious federal felonies. If the application is for an extension, it must set out the results obtained thus far or a reasonable explanation for the failure to obtain results under the previous warrant.[92]

82. The court must be satisfied that there is "*probable cause for belief*" that:[93]

    (a) An offence has been or is about to be committed;

    (b) Communications confirming the commission of the offence will be obtained;

    (c) Normal investigative procedures have been tried and failed or are unlikely to succeed;

    (d) The communications method is or will be used in connection with the commission of the offense.

83. The third of those criteria is not required for other types of investigatory warrant, such as a search warrant. As a result, interception warrants are sometimes referred to as "*super warrants*". The warrant shall not continue for longer than is necessary and may not be issued for more than 30 days.[94] In an emergency situation an interception may begin without an application to the court, if an application is made within 48 hours.[95]

84. The ordinary position under the WA 1968 is that an inventory of the fact of interception, dates and whether anything was intercepted is provided to the persons named in the order within 90 days of termination unless the authority can show "*good cause*" to

89 18 U.S.C § 2510(4).
90 As is the case in the United Kingdom, the precise boundary between data that is "*in the course of transmission*" and communications data is a complex area of some uncertainty.
91 18 U.S.C. § 2516 (1).
92 18 U.S.C. § 2518 (1)(f).
93 *Ibid*. at (3).
94 *Ibid*. at (5).
95 *Ibid*. at (7).

withhold that information at an *ex parte* hearing.[96] I was told, during my trip to the United States, that disclosure to the subject ordinarily occurs in the context of a criminal procedure. Those individuals who receive notification that they have had their communications intercepted but are not party to any criminal trial, rarely bring proceedings seeking damages. Such damages are capped in any event.

85. US Code Chapter 21 of Title 18, commonly referred to as the SCA, provides access for law enforcement to both contents and metadata that are stored on a Remote Computing Service. This provides computer storage or processing services to the public by means of an electronic communications system,[97] such as cloud storage. Access to the content of stored communications, without notice, is granted on the basis of a search warrant.[98] Access to stored material that does not include the content of communications may be granted on a similar basis.[99]

86. However, and importantly, a specified subset of non-content may be accessed by administrative subpoena without the scrutiny or authorisation of a court. Those data are: name, address, call records, length of service, types of service used, number used including temporarily assigned IP address, means and source of payment.[100] As a result, much of the most important metadata may be obtained without the permission of a court.

87. Furthermore, the SCA provides for access to metadata records, without judicial authorisation, where the Director of the FBI (or his designee) certifies that they are relevant to an authorised investigation to protect against international terrorism or clandestine intelligence activities. Those requests are known as "*National Security Letters*". The Director of the FBI may request, and a telecoms provider is required to provide, name, address, length of service and local and long distance toll billing records on that basis.[101]

88. An important distinction between US and UK law (as it currently stands) is that there is no requirement for service providers in the United States to store data beyond their own business needs. I was informed during my trip to the US that it was highly unlikely that Congress would consider legislation requiring service providers to retain or create data that they did not themselves need for business purposes (such as billing). However, telecommunications providers are required to retain data that they already produce and create such as: name, address, telephone number of the caller, telephone number called, date, time and length of a call.[102] If law enforcement agencies want access to material beyond that, or want access to other metadata, they are empowered to request that material is preserved, pending an application for access to that data.[103]

---

96 *Ibid*. at (8)(d).

97 18 U.S.C. § 2711(2).

98 If the data owner is put on notice, it may also be accessed via a court order, administrative subpoena or grand jury or trial subpoena 18 U.S.C. § 2703.

99 Search warrant, telemarketing fraud request or court order. It is important to note that for non-content subscriber records, no notice has to be given to the subscriber.

100 18 U.S.C. § 2703 (2).

101 18 U.S.C. § 2709 (b).

102 17 C.F.R. § 42.6.

103 E.g. 18 U.S.C. § 2704.

89. Finally PRA grants both federal and state law enforcement the right to make records of outgoing numbers from (pen register) and incoming calls (trap and trace) to a particular phone number pursuant to a court order.[104] The definition of a "*pen register*" was widened by the USA PATRIOT Act in 2001. It now includes a device which records "*signalling information"* that can record access to the internet and other network analysis devices.[105] The procedure for obtaining a court order is less onerous than the procedure for obtaining a warrant, both in terms of the standard of proof to be met and the level of detail that is ordinarily provided.[106] Court orders under the PRA last for up to 60 days. They do not provide a basis for gaining access to the contents of communications.

Gathering of foreign intelligence

90. FISA 1978 (as amended) authorises the electronic surveillance of foreign powers overseas - including groups engaged in international terrorism - and agents of foreign powers. Much of the material collected under FISA 1978 is gathered overseas or concerns the activities of non-US citizens in the mainland United States. However, a US person may also be an agent of a foreign power,[107] to the extent that they knowingly gather intelligence for a foreign power or engage in sabotage or terrorism on behalf of a foreign power.

91. FISA 1978 authorises broadly three kinds of data collection. First the traditional FISA 1978 process requires a Federal officer, with the approval of the Attorney General, to apply to the FISC, a bespoke federal court made up of eleven district court judges set up following reports of abuse by the intelligence agencies in the United States, for an interception warrant. Those eleven judges sit part time, at the court for one week stints on duty, where they read or hear warrant applications under FISA 1978. The Court has 10 full time staff members: five counsel to the Court and five administrative staff.[108]

92. The majority of applications are dealt with on the papers though I was informed that around 10% are dealt with following an oral hearing.[109] The judges can and do request that the individual who swore an affidavit in support of the application appears before them so that they can be asked questions by the judge. No special advocate can appear to make submissions in defence of the privacy interests in issue. The court has recently accepted an amicus brief from the Centre for National Security Studies on the question of bulk metadata production.[110] However, I am not aware of amicus counsel being instructed to make submissions in specific cases. Historically very few judgements of the FISC have been published. However, there has been a trend towards publication in recent years. A telecommunications provider, that is ordered to provide access to material, or a government body that has applied for a warrant may

104 18 U.S.C. § 3121.
105 18 U.S.C. § 3127 (3).
106 18 U.S.C. § 3122.
107 Defined as a citizen of the US, an alien with lawful permanent residence or a US corporation or unincorporated association.
108 The court does not publish details of its costs but the District Court Judges are not paid any additional salary for their FISC work.
109 In the calendar year 2013, the FISC received 1,655 applications under s 702, 178 applications for "*tangible things*" under s215 and the FBI applied for 14,219 National Security Letters.
110 http://www.fisc.uscourts.gov/sites/default/files/Misc%2014-01%20Order-1.pdf.

appeal a decision of the FISC to the United States Foreign Intelligence Surveillance Court of Review. In practice, such appeals are rare.

93. An application for a FISA 1978 warrant must specify the identity (if known) or a description of the specific target of the electronic surveillance. It must set out the facts and circumstances to support the belief that the target is a foreign power or agent of a foreign power and that the targeted facilities will be used by them.[111] The application must also set out the minimisation procedures in place to ensure that the correspondence of United States persons is not acquired, retained or distributed.[112]

94. The judge of the FISC must be satisfied that there is probable cause to believe that the elements above are satisfied (including that the target is a foreign power or agent of a foreign power). An order may be granted for up to 90 days.[113] FISA 1978 orders may be granted that authorise the interception of the communications of US citizens, to the extent that the FISC judge is satisfied that there is probable cause to find that that individual is an agent of a foreign power.

95. The second, more controversial, aspect of FISA 1978 arises out of a series of amendments to the Act introduced in 2008 (the FISA Amendment Act 2008 Section 702 allows the targeting of individuals "*reasonably believed to be located outside the United States to acquire foreign intelligence information*" without the same degree of judicial scrutiny.[114] Under s702, the Attorney General and the Director of National Intelligence may jointly authorise that targeting for a period of up to one year. Acquisition of data via this route may not intentionally target:

    (a) Any person known to be located in the United States;

    (b) A person outside of the United States in order to target a person reasonably believed to be in the United States;

    (c) A United States person reasonably believed to be outside the United States; or

    (d) Any communication as to which the sender and recipients are all known to be inside the United States.

96. The basic mechanics of s702 are:

    (a) The Attorney General and Director of National Intelligence draw up a certificate identifying categories of foreign intelligence that they wish to collect (for example email addresses of suspected terrorists overseas). Those certifications do not contain the level of specificity as to the individual targeted that is required under a normal FISA 1978 order;

    (b) The certification must set out the targeting procedures that will be used. They must be "*reasonably designed"* to ensure that the material acquired is "*limited to targeting persons reasonably believed to be located outside the United*

111 50 U.S.C. § 1804 (a).
112 See: 50 U.S.C. § 1801.
113 50 U.S.C. § 1805.
114 50 U.S.C § 1881a.

States." The certification must also attest that the Attorney General has adopted Guidelines to ensure compliance with the s702 framework.

(c) A judge of the FISC reviews the minimisation and targeting provisions of those certifications before they are implemented. They must be satisfied that the targeting procedures are "*reasonably designed*" to meet the objectives set out above.[115] The presiding judge writes an opinion setting out why he or she considers that the procedures meet that standard and also why they comply with the First Amendment right to free speech.

(d) However, the judge does not have to approve the targeting decisions: they do not have to satisfy themselves that the target (or targets) are a foreign power or agents of a foreign power.[116]

(e) The NSA have published a fact sheet on their minimisation procedures, which provides that inadvertently acquired communication of or concerning a US person must be promptly destroyed if it is neither relevant to the authorised purpose or evidence of a crime.[117]

97. The Inspector General assesses compliance with the procedural requirements and reports on them on an annual basis to Congress. The Attorney General also submits a report to Congress each year setting out the number of applications and extensions of s702 surveillance certificates and the number of those orders or extensions granted, modified or denied.[118] He also submits a semi-annual assessment to three Congressional select committees concerning all electronic surveillance under s702.[119]

98. Section 702 provided the basis for the US Government to carry out its PRISM and Upstream collection programs (described more fully at Annex 7 to this Report).

99. A third, and equally controversial, aspect of FISA 1978 is Subchapter IV: Access to Certain Business Records for Foreign Intelligence Purposes (known as s215). It provides that the Director of the FBI, or a designee, may make an application for an order requiring the production of any "*tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities*."[120]

100. An application under s215 should be made to the FISC and include a statement of facts showing that there are reasonable grounds to believe that the things sought are relevant to an authorised investigation.[121] If the court is satisfied that that is the case, it will issue an order that describes the tangible things that must be provided "*with sufficient particularity to permit them to be fairly identified*."

115 50 U.S.C. § 1881a (i) (2)(B)(i)
116 50 USC § 1881a (g).
117 https://www.fas.org/irp/news/2013/06/nsa-sect702.pdf.
118 50 U.S.C. § 1807.
119 50 U.S.C. § 1808.
120 50 U.S.C. § 1861(1).
121 *Ibid*. 1861(1) (b).

101. Section 215 has become controversial in the light of the disclosures in the Snowden Documents, when it became clear that the FBI had applied, on behalf of the NSA, for orders authorising the collection of nearly all call information generated by certain telephone companies in the USA. The NSA had then queried the database of information that resulted by enquiring for all calls to or from telephone numbers in respect of which there was a "*Reasonable Articulable Suspicion*" that it was associated with terrorism (the seed number). The NSA then operated a system known as contact chaining whereby all persons in contact with the seed number - the first hop - all numbers directly in contact with the first hop numbers (the second hop) and all numbers in contact with those second hop numbers as well (the third hop) could be accessed and stored.[122] The judges of the FISC had authorised that program pursuant to a series of 90 day orders.

102. Finally, EO 12333 provides an extra-statutory basis for the intelligence services to carry out interception of communications. It was first issued in 1981 and has been amended on three occasions since. Part 1 of EO 12333 sets out the various roles of the intelligence bodies in the United States. Part 2 includes a broad power to collect information. Comparatively little is known about the use of those powers. If it is relied upon as a basis for carrying out interception, the intelligence agencies may do so without judicial authorisation.

Oversight

103. The intelligence services in the United States are subject to multiple forms of oversight. In 2007 Congress established a Privacy and Civil Liberties Oversight Board to review and oversee civil liberties in the context of national security. The Board has published two report. Its first, in January 2014 concerned the "*section 215 program*" and held that it did not comply with the statute itself. In particular, the Board held that the program had been authorised by reference to counter-terrorism investigations in general, and not a specific authorised investigation (as required). They also expressed their serious reservations about whether or not it complied with the Constitution.[123] A second report in July 2014, concerning s702 concluded that certain historical programs "*push the program close to the line of constitutional reasonableness."*[124] However, they concluded that the program was, in broad terms, lawful. Both Houses of Congress also provide legislative oversight in the form of a permanent select committee on intelligence.

104. A separate President's Intelligence Oversight Board reports directly to the President on potential violations of the law committed by the Agencies. Many of the Agencies themselves also contain an Office of Inspector General, with a remit to review compliance internally.[125]

---

122 Following a change in 2014 the FISC now has to approve RAS determinations before contact chaining may be carried out.

123 http://www.fas.org/irp/offdocs/pclob-215.pdf. That was a view shared by the President's Review Group on Intelligence and Communications Technologies, p. 85. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

124 http://www.pclob.gov/library.html page 9.

125 17th Report of Session 2013-14, HC231 (May 2014), p. 92.

Annex 16: POTENTIAL USE OF TRAFFIC DATA BY LOCAL AUTHORITIES **(9.83 above)**

1. The information in this Annex derives from evidence to the Review from Hampshire County Council officers, March 2015.

Cold calling fraud

2. In April 2012 Mr V was arrested at a house where a consumer had been defrauded of a considerable amount of money. Other persons ran away and could not be identified.

3. From itemised billing checks on Mr V's telephone number, it was established that Mr V had been in regular contact with a Mr A. Itemised billing for Mr A's phone number showed a pattern of contacts with Mr V.

4. Some time later Mr A was arrested, but on interview he denied being present at the address and he claimed that someone else had asked him to cash a cheque that had been written by the consumer. Nothing could be proved to the contrary.

5. Only Mr V was able to be prosecuted for the fraud offences and he was eventually given a suspended sentence of 15 months imprisonment plus community service. He was also given a 7 year Criminal Anti Social Behaviour Order [**CRASBO**] banning him from being involved in cold calling anywhere in England and Wales.

6. All that could be proved against Mr A was a money laundering offence and he was just given a sentence of 140 hours community service. The local authority was unable to apply for a CRASBO against him, as they could not place him at the scene.

7. Had the local authority been able to access traffic data they would have checked location data for Mr A's phone, which would have been likely to show he had been in the vicinity at the consumer's house at the time of the offences. If this had been established this would have enabled them to prosecute him for the fraud offence and quite possibly to have used a conspiracy charge involving both men. If there had been a successful fraud prosecution, this would have resulted in a CRASBO being obtained against Mr. A. The CRASBO would have protected vulnerable consumers in general, since he would be liable to arrest if he was caught cold calling anywhere, even if no fraud was provable.

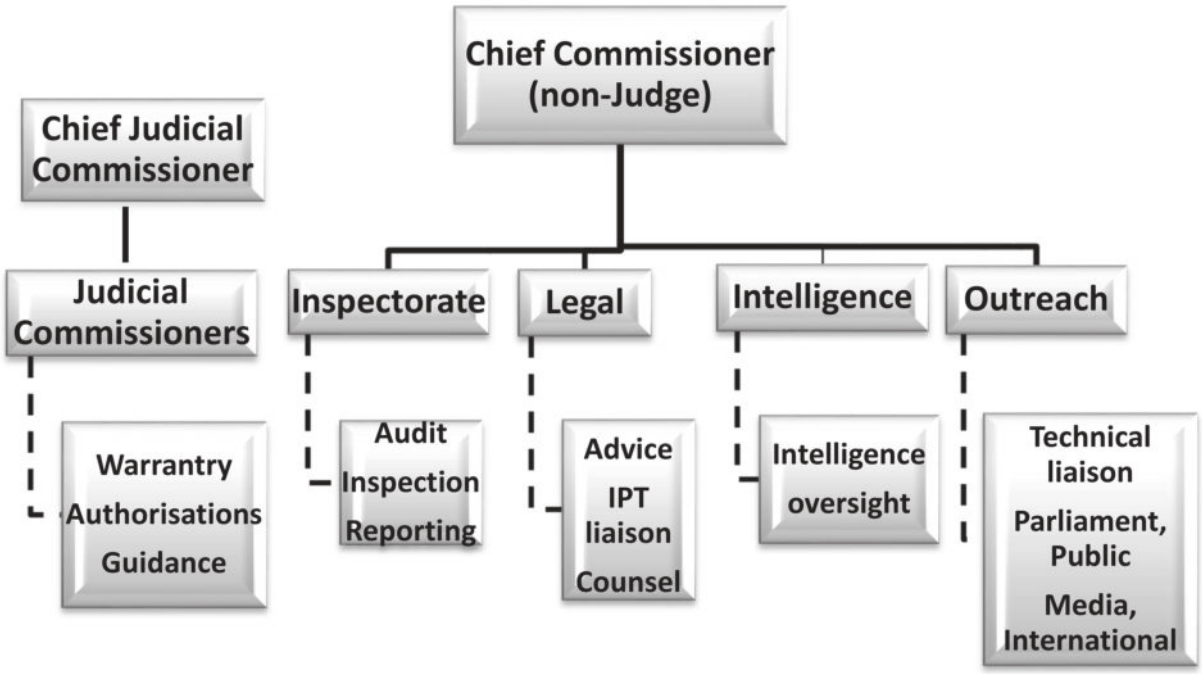
Counterfeit goods

8. In a number of cases, a local authority has seized counterfeit goods from persons who are selling them locally, but appear to be obtaining them from other persons further up the distribution chain. The defendants have claimed not to know the name or phone number of their supplier, because he just rings them when he is about to deliver more stock. Consequently the local authority is usually only able to prosecute the person from whom the items were seized. If they were able to access traffic data they could use this to obtain incoming calls data for the defendant's phone to try to identify the supplier. This would otherwise not be possible as the defendant was not making phone calls to the supplier. Rather than just prosecuting the persons at the bottom of the

distribution chain, they would be able to prosecute the distributors who would also be supplying counterfeit goods to other persons in the locality and making greater profits.

Annex 17: Independent Surveillance and Intelligence Commission (ISIC) Model A (14.100 above)

Annex 18: Independent Surveillance and Intelligence Commission (ISIC) Model B (14.100 above)



ISBN 978-1-4741-1945-0