RESPONSE OF PRIVACY INTERNATIONAL TO THE CONSULTATION ON THE GOVERNMENT'S PROPOSED RESPONSE TO THE RULING OF THE COURT OF JUSTICE OF THE EUROPEAN UNION ON 21 DECEMBER 2016 REGARDING THE RETENTION OF COMMUNICATIONS DATA

Index:

A. About Privacy International

1. Privacy International was founded in 1990. It is a leading charity promoting the right to privacy across the world. It focuses, in particular, on ensuring that the collection and use of data is carried out within the law and is accompanied by strong and appropriate safeguards for data retention regimes.

2. Privacy International has been a party to most of the substantial Investigatory Powers Tribunal, Court of Appeal and European Court of Justice ["CJEU"] cases in the last five years which have dealt with issues concerning communications data.

3. Privacy International intervened in *Tele2 Sverige AB v Post-och telestyrelsen (*Case-203/15) and *R (Watson) v Secretary of State for the Home Department* (Case C-698/15), which has resulted in the landmark ruling by the European Court of Justice and ultimately this consultation. Privacy International together with Open Rights Group, argued in particular, that wholesale and indiscriminate retention of data is not permissible and violates European Union law.

4. Privacy International achieved success in *Privacy International v Secretary of State for the Foreign and Commonwealth Affairs & Ors* [2016] UKIPTrib 15/110/CH where the Tribunal held that the obtaining of Bulk Communications Data pursuant to section 94 Telecommunications Act 1984 had not been lawful at domestic law; and that neither the obtaining of Bulk Personal Datasets nor of Bulk Communications Data complied with Article 8 of the ECHR prior to their avowal in March / November 2015, by virtue of their lack of foreseeability to the public and in relation to BCD, the lack of adequate oversight by the independent Commissioners.

5. Privacy International has litigated or intervened in cases implicating the right to privacy and relating to mass surveillance including communications data retention and access, in the courts in Europe, including the European Courts of Human Rights, and in the United States of America. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect privacy.

6. In accordance with those aims, Privacy International has intervened in Court in cases including that relevant to this consultation, being *Watson, Brice & Lewis v Secretary of State for the Home Department* [Case No.C-698/15], in addition: *S and Marper v UK (*App. Nos 30562/04 and 30566/04), *Tretter and others v Austria* (App no. 3599/10), and *Breyer v Germany* (App. No 5000001/12);

Khadija Ismayilova v Azerbaijan (Application no. 65386/13). Outside of Europe and the UK, Privacy International has intervened in *Luis Fernando Garcia Munoz and Bosque David Inglesias Guzman v Mexico; People's Solidarity for Participatory Democracy v Republic of Korea; Naperville Smart Meter Awareness v Naperville* [Case No.16-3776]; *United States v Levin* [Case No.16-1567]; *In the matter of the search of Apple iPhone seized during the execution of a search warrant on a black lexus IS300* (Apple v FBI).

7. Privacy International is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

B. The consultation

8. The changes introduced by the new Communications Data Draft Code of Practice and the Data Retention and Acquisition Regulations 2018 affect Parts 3 and 4 of the Investigatory Powers Act 2016.

> "Section 2 of this code provides guidance on the procedures to be followed when **acquisition** of communications data takes place under the provisions of Part 3 of the Act.
>
> Section 3 of this code provides guidance on the procedures to be followed when communications data is **retained** under Part 4 of the Act."[1]

9. This response seeks to address comments made in the consultation document[2]; Draft Communications Data Code of Practice[3]; Draft Regulations amending the Investigatory Powers Act[4].

---

[1] Communications Data DRAFT Code of Practice, para 1.1

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/663668/November_2017_IPA_Consultation_-_consultation_document.pdf

[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/663675/November_2017_IPA_Consultation_-_Draft_Communications_Data_Code_of_Pract....pdf

[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/663677/November_2017_IPA_Consultation_-_Draft_regulations_amending_the_IP_Act.pdf

10. Due to the length of the documents and the short consultation period we are unable to provide a response to the Case Studies, Draft Impact Assessment and Communications Data Factsheet.

11. Privacy International have previously responded to the "The Home Office Investigatory Powers Act 2016 Consultation On The Draft Codes of Practice" on 4 April 2017 and the secret consultation on the Draft Investigatory Powers (Technical Capability) Regulations 2017. This response should be read together with those responses, which are provided with this response.

12. Privacy International responded throughout the passage of the Investigatory Powers Bill to a number of consultations including: Science and Technology Committee; Joint Committee on the Draft Investigatory Powers Bill; Joint Committee on Human Rights; House of Lords review of bulk power. We maintain the submissions made in those documents, many of which relate to issues raised by this consultation, and can provide them on request if required.

C. Introduction

13. The consultation is in response to the judgment in *Tele2 Sverige AB v Post-och telestyrelsen (*Case-203/15) and *R (Watson) v Secretary of State for the Home Department* (Case C-698/15) ["Watson judgment"].

14. The case concerned section 1 and 2 of DRIPA and the Data Retention Regulations 2014. This contained the legislative scheme concerning the power of the power of the Secretary of State to require communications service providers to retain communications data. Part 3 of the Counter-Terrorism and Security Act 2015 amended DRIPA so that an additional category of data – that necessary to resolve Internet Protocol addresses – could be included in a requirement to retain data.

15. The European Court of Justice held that the ePrivacy Directive (2002/58/EC) when read in light of the EU Charter of Fundamental Rights, prohibits national legislation from imposing data retention obligations unless it is 'strictly necessary' for the purpose of fighting 'serious crime' and that measures allowing for 'general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication' are not permitted. The European Court of Justice held that law enforcement agencies can only access the retained data where it is 'strictly necessary' for the purpose of fighting serious crime and where such access has been approved following a prior review by a court or independent authority.

16. Privacy International intervened in the case together with Open Rights Group and made submissions that both an obligation to retain and an obligation to disclose or grant access to personal data are data-processing activities covered by the ePrivacy Direction and the Data Protection Directive.

17. Privacy International believes that the Government's Draft Code of Practice for Communications Data and the proposed amendments to Parts 3 and 4 IPA fail to fully implement the European Court of Justice's judgment in *Tele2 Sverige AB v Post-och telestyrelsen (*Case-203/15) and *R (Watson) v Secretary of State for the Home Department* (Case C-698/15), which specified a number of EU law requirements a regime governing the retention and acquisition of communications data must meet.

18. The Government has sought to circumvent express mandatory safeguards identified in the court judgment by:
    a. Proposing that entity data does not form part of communications data to which the Watson judgment applies;
    b. Removing the application of the judgment from 'data held for business purposes'.
    c. Re-defining serious crime for retention and access purposes;
    d. Avoiding independent judicial oversight;

19. In addition, the consultation has failed to identify issues concerning:
    a. Transitional provisions of the Investigatory Powers Act 2016 which result in unlawful access and retention;
    b. The broad definition of telecommunications operators which significantly expands those upon whom data retention notices can be served.

20. Cumulatively, these actions taken by the Government and its proposals undermine the judgment and provide for a data retention regime which is general and indiscriminate. The judgment stated:

> Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, **must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate**

retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

[emphasis added]

21. The CJEU gave clear and unequivocal guidance as to the requirement of EU law in relation to data retention regime, stating as follows (emphasis added):

"102: Given the seriousness of the interference in fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure.

103. Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purpose of that fight.

112. Having regard to all the foregoing, the answer to the first question referred to in Case C-203/15 is that Article 15(1) of the Directive 2002/58, read in light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

22. In A Question of Trust, David Anderson QC stated[5] that "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.
    (b) This in turn requires knowledge at least in outline of what powers are liable to be used, and visible authorisation and oversight mechanisms in which the wider public, as well as those already initiative into the secret world, can have confidence.
    (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.

23. He stated that obligatory data retention requires service providers to retain and make available valuable communications data relating to effectively the whole population. He goes on to emphasise the need for accessible and foreseeable laws; powers exercised only when strictly necessary and proportionate; for a clear and comprehensive system of authorisation, monitoring and oversight; and for effective remedy.

24. In our submission, the proposals in the Consultation which relate to amendments to the Investigatory Powers Act 2016 and the Draft Code of Practice for Communications Data not only fail to implement the judgment but provides for a law that is neither accessible nor foreseeable; where powers are not limited to exercise when strictly necessary and proportionate and where the system for authorisation, monitoring and oversight is opaque. Finally, the failure to give due consideration or attempt to formulate a system of notification undermines the basic requirement for effective remedy.

25. The attempt of the Government to undermine the judgment of the CJEU will have repercussions for an **adequacy decision** in relation to data transfers. Post Brexit, for third countries looking to exchange data with the EU, the GDPR provides for two broad options. The first would be for the UK to receive an 'adequacy decision' from the European Commission certifying that it provides a standard of protection which is "essentially equivalent" to EU data protection standards.

[5] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf para 13.3

26. However, as noted by the House of Lords Brexit Committee[6]:

> *"When considering an adequacy decision, the European Commissioner will look at a third country's data protection framework in the round, including national security legislation. If the UK were to seek an adequacy decision, the UK would no longer be able to rely on the national security exemption in the Treaty on the Functioning of the European Union that is currently engaged when the UK's data retention and surveillance regime is tested before the Court of Justice of the European Union.*
>
> *113. Continuing UK alignment with the EU data protection laws could come into tension with the Government's preferred approach to data retention and surveillance for national security purposes. While the UK remains a member of the EU, national security is the sole responsibility of each Member State, as outlined in the TFEU (article 4.2). However, the boundaries between Member State competence over national security and EU competence over data protection and retention are increasingly being tested before the CJEU."*

27. Thus, if the UK government continue to seek to undermine the decision of the CJEU in pursuing the proposals set out in this consultation and failing to give effect to the mandatory safeguards, this together with other national security measures, will threaten an adequacy decision.

28. We do however, note one aspect of transparency this consultation has highlighted. At page 14 of the Consultation document is states that:

> *"Section 90(13) of the Act requires the Secretary of State to keep a data retention notice under review, and revoke a notice where retention is no longer necessary and proportionate, or vary it where retention of communications data relating to a particular service offered by the provider is not necessary and proportionate. Law enforcement has engaged with over 700 telecommunications and postal operators in the past two years, less than 25 of these are or have ever been subject to a data retention notice."*

29. Given the Government are prepared to state how many operators are receiving data retention notices in the consultation document, this demonstrates that a publicly available central register documenting the

[6] House of Lord, European Union Committee, 3rd Report of Session 2017-19 "Brexit: the EU data protection package".

number of telecommunications operators served with notices can be maintained.

30. **We recommend the Investigatory Powers Commissioner maintain a publicly available central register documenting the number of telecommunications operators served with notices, to be established without delay.**

D. Transitional provisions of the Investigatory Powers Act 2016 – unlawful access and retention

31. 10 days after the Grand Chamber gave the Watson judgment (on 31 December 2016) the sunset clause in section 8(3) DRIPA 2014 took effect. However, existing DRIPA retention notices have been continued by Schedule 3, para 3 of the IPA 2016.[7]

32. On 15 December 2016, the Defendant made the Investigatory Powers Act 2016 (Commencement No.1 and Transitional Provisions) Regulations 2016 ("IP Act Commencement Regulations") pursuant to sections 270 and 272 IP Act. The IP Act Commencement Regulations brought into force the communications data retention provisions in the IPA shorn of the provisions regarding oversight and review, with effect from 30 December 2016.

33. Under the transitional provisions of the IP Act Commencement Regulations, Schedule 9, paragraphs 3, retention notices issued under the Data Retention

[7] The Explanatory Note to SI No.1233 (C.85) states: Regulation 2 brings into force the repeal of sections 1 and 2 of the Data Retention and investigatory Powers Act 2014 (c.27), which provide for communications data retention. Schedule 9 of the 2016 Act provides that a retention notice given under the 2014 Act continues to have effect for a period of 6 months from the 30th December ("the transitional period") as if it were a notice given under Part 4 of the 2016 Act.

Schedule 9 (3) Retention of communications data

(1) A retention notice under section 1 of DRIPA which is in force immediately before the commencement day is to be treated, on or after that day, as a retention notice under section 87 of this Act…

(2) In particular

a. Anything which, immediately before the commencement day, is in the process of being done by virtue of, or in relation to, a retention notice under section 1 of the Act 2014 may be continued as if being done by virtue of, or in relation to, a retention notice under section 87 of this Act, and

b. Anything done by virtue of, or in relation to, a retention notice under section 1 of the Act of 2014 is, if in force or effective immediately before the commencement day, to have effect as if done by virtue of, or in relation to, a retention notice under section 87 of this Act so far as that is required for continuing its effect on or after the commencement day.

Regulations 2014 ("DRIPA") will continue to have effect and will be deemed to have been give under s.87 of the Investigatory Powers Act 2016 ("IPA"), for a transitional period of 6 months. The transitional provisions make clear (Schedule 9, paragraph 2) that the DRIPA data retention regimes is to be replicated under the IPA:

> *"(a) anything which, immediately before the commencement day, is in the process of being done by virtue of, or in relation to, a retention notice under section 1 of the Act of 2014 may be continued as if being done by virtue of, or in relation to, a retention notice under section 87 of this Act, and*
>
> *(b) anything done by virtue of, or in relation to, a retention notice under section 1 of the Act of 2014 is, if in force or effective immediately before the commencement day, to have effect as if done by virtue of, or in relation to, a retention notice under section 87 of this Act so far as that is required for continuing its effect on or after the commencement day."*

34. Until the provisions of the IPA which provide for access to that data are brought into force, the Defendant intended the existing arrangements under s.22 RIPA 2000 to apply.

35. In light of the transitional provisions in the IP Act Commencement Regulations noted above, the IPA 2016 transitional provisions thus required all DRIPA retention notices to be replaced by 30 June 2017.

36. However, this means that data held under DRIPA notices, which must be retained for up to a year, can be retained and accessed, under the DRIPA regime, until 30 June 2018.

37. As noted above, the IPA Commencement Regulations brought into force the communications data retention provisions in the IPA shorn of the provisions regarding oversight and review, with effect from 30 December 2016. Thus, the additional safeguards required by IPA 2016 were excluded, pursuant to Schedule 9, paragraph 3(1) of the IPA 2016 (i.e. prior approval by a Judicial Commissioner). This is for all existing DRIPA notices deemed to be converted into IPA 2016 notices as at December 2016, which may have survived until June 2017.

38. The position is therefore that the retention notices granted under DRIPA are continued, without the additional safeguard in the IPA 2016, for a period. The retention notices are deemed to be IPA 2016 notices, but the quality of

safeguard governing the issue of the notices and access to the data re unchanged and reflect those in DRIPA.

39. Noting the findings in the judgment of the Court of Justice of the European Union on 21 December 2016 ("the Watson judgment") cited below regarding judicial oversight, and the amendments to Parts 3 and 4 as a result of the judgment, notices issued under DRIPA have a continuing effect and data retained under them, as a result of the IPA 2016 transitional provisions, will continue to be held, and DRIPA data will be regularly access, unlawfully, until 30 June 2018.

40. **The consultation fails to appreciate that whilst DRIPA notices may have been replaced, the underlying data held under old notices remains available for access point. We recommend the Government seek to rectify this ongoing unlawfulness.**

E. The roles of Codes of Practice

41. As per the judgment of the Court of Justice of the European Union on 21 December 2016 ("the Watson judgment") in joined cases C-203/15 and C-698/15 *Tele2 Sverige AB. V Post-och telestryrelesen and Secreatry of State for the Home Department v Tom Watson & others,* a Code of Practice is not the appropriate place to provide additional rules regarding the government's surveillance powers, as the Code of Practice is not legally binding. Instead, primary legislation must serve this purpose:

> 117. Further, since the legislative measures referred to in Article 15(1) of Directive 2002/58 must, in accordance with recital 11 of that directive, 'be subject to adequate safeguards', a data retention measure must, as follows from the case-law cited in paragraph 109 of this judgment, lay down clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law.

42. Codes are important tools for clarification of existing authorisations and obligations conferred by law. **However, the Code must merely provide guidance for authorities but cannot replace the law or be used to generate new powers that were note otherwise provided by Parliament.**

43. In addition, we are concerned that §1.12 of the Draft Communications Data Code of Practice permits the issuing of advice directly to public authorities, telecommunications operators and postal operators, in addition to the Code. This undermines transparency. It is unclear whether the Code takes precedence over these secret notices.

44. §2.85 of the Draft Communications Data Code of Practice permits the development of definitions in the Act in secret. This is unacceptable.

> *"The Home Office may issue further guidance to telecommunications operators, postal operators or public authorities, on how the definitions in the Act apply."*

45. **We recommend that all guidance and definitions are publicly available. Should there be a need for non-public documents for telecommunications operators, which must be subject to independent oversight and limited to specific reasons. The formulation of these limited reasons must be subject to public consultation prior to implementation.**

46. **We recommend that the Investigatory Powers Commissioner ensures that definitions are not developed in secret.**

F. Who is a Telecommunications operator

47. The definition as to who falls under the definition of Telecommunications Operators (previously referred to as Communication Service Providers (CSPs) or Public Electronic Communication Networks (PECNs)) has been expanded by the Investigatory Powers Act 2016 to the point that it is so broad as to be meaningless.

48. Prior to the Investigatory Powers Act, legislation[8] referred to 'public' telecommunications operators. The Investigatory Powers Act has dropped the 'public' and refers simply to telecommunications operators. A telecommunications operator is defined at section 261(10) of the Act as a person who "(a) offers or provides a telecommunications service to persons in the UK, or (b) controls or provides a telecommunications system" in or controlled from the UK.

[8] E.g. Regulation of Investigatory Powers Act 2000, Data Retention and Investigatory Powers Act 2014

49. At 261(11) a "Telecommunications service" is "*any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system"* and at 261(13) a "Telecommunications system" is *"a system . . . that exists . . . for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy".*

50. The Draft Communications Data Code of Practice states:

> *"2.4 The definition of a telecommunications operator also includes application and website providers but only insofar as they provide a telecommunications service. For example, an online market place may be a telecommunications operator as it provides a connection to an application/website. It may also be a telecommunications operator if and in so far as it provides a messaging service.* ***This means that numerous businesses will be considered telecommunications operators in respect of some of their work is unrelated to telecommunications services or telecommunications systems.*** *It can therefore sometimes be difficult for a relevant public authority to determine whether they need an authorisation under Part 3 of the Act to acquire the information they are interested in."*
>
> *"2.12 Telecommunications operators may also include those persons who* ***provide services where customers, guests or members of the public are provided with access to communications services that are ancillary to the provision of another service, for example in commercial premises, such as hotels or public premises such as airport lounges or public transport.*** *Such telecommunications services may be provided by the overall service provider or by another telecommunications operator as a partner or on their behalf. In the circumstances where it is impractical for the data to be acquired from, or disclosed by, the service provider e.g. the hotel, restaurant, library or airport lounges, or where there are security implications in doing so, the data may be sought from the telecommunications operator which provides the communications service offered by such hotels, restaurants, libraries and airport lounges. Equally, circumstances may necessitate the acquisition of communications data from such organisations, for example, where a hotel is in possession of data identifying specific telephone calls originating from a particular guest room."*

[emphasis added]

51. The Draft Communications Data Code of Practice states at §2.2 that *"The definitions of 'telecommunications service' and 'telecommunications system' in the Act are intentionally broad so that is remains relevant for new technologies"* We do not agree that it is justifiable to use such *'intentionally broad'* definitions, solely on the basis that *'it remain[s] relevant for new.'*

52. We submit that this lack of precision and 'intentionally broad' approach raises issues of legality. The interference with the right to privacy needs to comply with the principle of legality, including the requirement of foreseeability of the scope of its application - "a norm cannot be regarded as a law unless it is formulated with the sufficient precision to enable the citizen to regulate his conduct; he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail".[9]

53. In the context of the vast quantities of data which this could entail, not only is the 'intentionally broad' definition of a telecommunications operators a cause for concern, the lack of clarity as to who falls into this category and the method to determine basic safeguards appear the subject of confusion. We further note as set out below that the re- definition of 'serious crime' to include what is normally not classed as 'serious crime', further impact on the quantities of data that will be retained.

54. The Draft Communications Data Code of Practice sets out at §2.5 – 2.12 that since a *"§2.5 … large number of companies are telecommunications operators for the purposes of the Act, but they will also provide other services. It will sometimes be difficult for a relevant public authority to determine whether the information they are seeking is communications data held in relation to a telecommunications service and therefore whether this code is relevant to an authorisation under Part 3 of the Act will be required."*

55. There is a lack of clarity in the Code and in the Act as to what powers would be used if data was considered not to fall under the definition of communications data held in relation to telecommunications service and what safeguards are in place, particularly if there are classification errors.

[9] Sunday Times v. the United Kingdom, European Court of Human Rights, App. No. 6538/74, 26 Apr. 1979, para. 49.

56. In cases where the public authority is unsure, they should contact the Single Point of Contact (SPoC). A SPoC is not independent of the public authority but, as set out at §76 IPA:

> *"76. Use of a single point of contact*
> *(4) A person is acting as a single point of contact if that person –*
> *(a) is an officer of a relevant public authority, and*
> *(b) is responsible for advising –*
> *(i) officers of the relevant public authority about applying for authorisations, or*
> *(ii) designated senior officers of the relevant public authority about granting authorisations."*

57. This is an issue which applies as whole to the IPA and to previously consulted upon draft Codes. We have noted in our submission on the consultation on the other Draft Codes of Practice:

2.10. The EI Code demonstrates the broad reach of the definition stating that "telecommunications operator" also includes:

2.10.1. *"application and website providers . . . insofar as they provide a telecommunication service. For example an online marketplace may be a telecommunications operator if it provides a connection to an application/website".* [§2.12]

2.10.2. *"a telecommunications operator if and in so far as it provides a messaging service."* [§2.12]

2.10.3. *"those persons who provide services where customers, guests or members of the public are provided with access to communications services . . . ancillary to the provision of another service . . . for example in commercial premises such as hotels or public premises such as airport lounges or public transport."* [§2.13]

2.11. The Bulk Acquisition Code adds that:

2.11.1. *'...any service which consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunication system is included with the meaning of 'telecommunication service'. Internet-based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition.'* [§2.4]

2.12. The Autumn 2016 version of the Bulk Acquisition Code had other examples. It is not clear why these have been deleted:

2.12.1. *"In circumstances where it is impractical for the data to be acquired from, or disclosed by, the service provider, or where there are security implications in doing so, the data may be sought from the CSP which provides the communications service offered by such hotels, restaurants, libraries and airport lounges. Equally circumstances may necessitate the acquisition of communications data for example where a hotel is in possession of data identifying specific telephone calls originating from a particular guest room."* [§2.7]

2.13. In light of the above it is misleading for the Bulk Acquisition Code, for example, to give the impression that those to whom obligations apply, is limited - *'The obligations ... apply to telecommunications operators only...'*

58. We recommend the government:

a. Review the definition of telecommunications operator, provide one that is 'foreseeable' and not 'intentionally broad';
b. The need for independent oversight as to whom falls within the definition of a telecommunications operator, by the Investigatory Powers Commissioner;
c. To maintain a central list be maintained and updated on a regular basis by the Investigatory Powers Commissioner's Office ("IPCO");

d. Oversight and review of the practices set out at §2.5 – 2.12 and decisions made by the SPoC. In order for effective review, records must be kept of these activities, decision making and errors.

G. The intrusive nature of communications data

59. At a meeting with the Home Office in November 2017, on the day this consultation was launched, during a discussion between Privacy International and other NGOs, a senior Home Office representative voiced the position that he could not understand the level of our concern with the proposals, given that this consultation and data retention in Parts 3 and 4 concerns 'communications data'. The position of the Home Office representative appeared to be, it's not 'content' so why the fuss.

60. It is common ground that bulk collection of content would be a deprivation of the right to privacy. That is an inexcusable or unjustifiable step too far. Repeatedly the Government whether in litigation or legislating, has emphasised that they are not taking content in bulk. Content is the forbidden ground.[10]

61. This has resulted in the Government seeking to explain, for example, what parts of an email would constitute content and meta data. Within the Investigatory Powers Act it has led to the creation a plethora of definitions and types of communications data, narrowing what falls within the definition of 'content' and thus increasing the volume of data which can be subject to data retention and access powers.

62. However, that communications data can reveal private information on individuals as much as content data has been long recognised by Courts and expert bodies.

63. The essence of the truth grappled with by the European Court of Justice is that this somewhat old-fashioned distinction between content and communications data or traffic data is, in fact, no longer fit for purpose as some kind of formalistic distinction. The European Court of Justice say, entirely realistically, entirely accurately, that communications data, when collected in aggregate about one or a number of individuals is potentially no less sensitive, in their words, than the actual content.

[10] Although it has been acknowledged that bulk personal datasets contain content.

64. The boundary between content and communications, which may have worked pre-internet, in a world of intermittent phone calls and letters sent by post or telegram, simply becomes unworkable or unsafe in an age of 24-hour browsing, mailing, messages, instant apps, where that replaces conventional social interaction. When people live their lives online, where their smart phone is a tracking device of their every movement, the boundary is simply unsafe because of the welter of information derivable from communications data. It tells you everything, or nearly as much as the content itself.

65. Communications data includes, but is not limited to, visited websites, email contacts, to whom, where and when an email is sent, map searches, GPS location and information about every device connected to every wifi network in the United Kingdom, which includes Smart Tech, such as Nest, iKettle, Smart Barbie, Amazon Echo and others.

66. In the UK, we have one of the highest rates of internet shopping in the world[11]. We have one of the highest rates of penetration of smart phones in the world[12]. We take our TV and our entertainment from internet services like Netflix, Apple TV, Amazon Prime, You Tube, all of which is traceable and trackable via communications data.

67. A visit to an IP address, hosting a medical self-diagnosis website, followed by a visit to your GP's website, followed by a telephone call to an oncologist, followed by an appointment with a private client solicitor and then a hospice may well reveal that the person in question has terminal cancer.

68. Patterns of call behaviour to particular competitors, lawyers and then bankers and then accountants might be entirely dispositive in showing that a takeover is in prospect in relation to a particular company.

69. Communications data, is massively valuable. It is massively valuable in the hands of the state, but it also liable to misuse and a valuable target for theft, because one can see very readily how the blackmailer or the commercially unscrupulous, if they can use or get their hands upon such material, may use it in an ulterior way.

70. Further, the 21st century has brought with it rapid development in the technological capabilities of Governments to acquire, extract, filter, store, analyse and disseminate the communications of whole populations. The

[11] http://www.bbc.co.uk/news/business-39655039

[12] https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/

means of analysing the information have improved exponentially due to developments in automated machine learning and algorithmic designs.

71. That is the backdrop against which we have to assess risk of data retention powers. Not, as the Home Office appear to believe, that communications data is not intrusive.

72. As stated in Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); *Secretary of State for the Home Department v. Tom Watson et. al.* (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016):

> *"99. That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, 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. In particular, that data provides the means... of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."*
>
> [emphasis added]

73. The UNHCRC has stressed[13] that the distinction between the seriousness of interception of metadata and content is "not persuasive" and "any capture of communications data is potentially an interference with privacy […] whether or not those data are subsequently consulted or used." The mere fact of such capture may indeed have a "potentially chilling effect on rights, including those to free expression and association". The Commissioner concluded that "[m]andatory third-party data retention […] appears neither necessary not proportionate (paragraph [26] at p.9).[14]

74. The UN Human Rights Council noted, in a resolution adopted by consensus, "certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and

[13] In its report published on 30 June 2014, *"The right to privacy in the digital age"* (A/HRC/37), see fn.6.

[14] See also the report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson QC, UN doc. (A/69/397) at [55] (**Annex 7**).

can give an insight into an individual's behaviour, social relationships, private preferences and identity" (A/HRC/RES/34/7)

75. Further, as the Council of Europe's Commissioner has noted, "extensive research has failed to show any significant positive effect on clear-up rates for crime, and especially not for terrorism-related crime, as a result of compulsory data retention."[15] As he stressed, metadata can be "unreliable and can unwittingly lead to discrimination on grounds or race, gender, religion or nationality. These profiles are constituted in such complex ways that the decisions based on them can be effectively unchallengeable: even those implementing the decisions do not fully comprehend the underlying reasoning"[16].

76. The sheer volume of retained data will be huge.

77. Requiring telecommunications operators to retain all of our revealing and personal data for twelve months treats us all as suspects, undermining the trust we place in government to only exercise its power to intrude upon our personal lives in the most limited and necessary of circumstances.

[15] https://rm.coe.int/16806da51c page 113
[16] https://rm.coe.int/16806da51c page 8

H. Communications Data: events and entity data

78. The Government has sought to suggest that the CJEU judgment does not apply to communications data which it has defined as 'entity data'. In doing so, it exempts this category of communications data from essential safeguards mandated by the judgment. We submit that this attempt to circumvent the findings of the CJEU is unlawful.

79. The consequences of this manoeuvring are that requests for 'entity data' are not limited to cases involving serious crime; and requests for entity data may be authorised at a lower level within public authorities.

80. The Government in the consultation paper asserts that:

> *"The CJEU judgment refers to only certain types of communication data – traffic data and location data, as defined in Directive 2002/58/EC ("the ePrivacy Directive"). The definitions of "traffic data" and "location data' in the ePrivacy Directive are as follows:*
>
> > *"'Traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.*
> > *'Location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic service.""*

81. The Government goes on to assert that the judgment does not apply to entity data:

> *"The Government's view is that data covered by the definition of "events data" in section 261 of the IPA includes the data covered by the definitions of "traffic data" and "location data" in the ePrivacy Directive. Accordingly, the CJEU's judgment should be read as applying to "events data"* ***but does not apply to the retention and acquisition of "entity data" within the meaning of section 261.***
>
> [emphasis added]

What is events and entity data?

82. The consultation papers states in the section 'Response to the judgment' that:

"Application of the judgment to entity data
The IPA updated the definitions of communications data to reflect changes to the way in which communications services operate. The definition of communications data in the IPA creates two distinct categories of data: entity data and events data. The definition of entity data covers information which would previously have been classed under RIPA as subscriber data, while the definition of events data covers information previously classed under RIPA as traffic and service use data."

83. The definitions are contained in section 261 of the Investigatory Powers Act and state as follows:

> *"'Entity data' means any data which –*
> *(a) Is about –*
> *i. An entity,*
> *ii. An association between telecommunications service and an entity, or*
> *iii. An association between any part of a telecommunication system and an entity,*
> *(b) Consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location), and*
> *(c) Is not events data.*
>
> *'Events data' means any data which identifies or describes an event (whether or not by reference to its location) on, in, or by means of a telecommunications system where the event consists of one or more entities engaging in a specific activity at a specific time."*

84. The consultation paper states:

> 'Subscriber data – defined in RIPA as information held or obtained by a communications service provider about persons to whom they provide or have provided a communications service. Those persons will include people who are subscribers to a communications service without necessarily subscribing to it. The IPA defines this data as a type of **'entity data'.**
>
> Entity data – defined in the IPA as information about a person or thing, and about links between a telecommunications service, part of a telecommunication system and a person or thing, that identify or

describe the person or thing. For example, individual communication devices such as phones, tablets and computers are entities, as are the links between a person and their phone, which would include billing payments, who the account holder is, and information about the apparatus used by, or made available to the subscriber or account holder.'

Communications data to which the judgment applies

85. To gain a full perspective on the artificial attempt to exclude aspects of communications data, for the sole reason of avoiding independent judicial oversight and to gather more data than that permitted by the 'serious crime' requirement, it is necessary to consider the origins of the CJEU judgment to which this consultation relates.

86. The CJEU judgment in the Watson case, related to the mandatory safeguards set out in the Digital Rights Ireland judgment. The Digital Rights Ireland case challenged the Data Retention Directive, Directive 2006/24/EC.

87. The Data Retention Direction, Directive 2006/24/EC[17] itself very clearly relates to all types of communications data. The only type of data it explicitly excludes, is content data.

(13) This Directive relates only to data generated or processed as a consequence of a communication or communication service and does not relate to data that are the content of the information communicated…Data generated or processed when supplying the communication services concerned refers to data which are accessible. In particular as regards the retention of data relating to Internet e-mail and Internet telephony, the obligation to retain data may apply only in respect of data from the providers' or the network providers own services.

Article 1
2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communication, including information consulted using an electronic communication network.

Article 2: Definitions

[17] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

2.(a) 'data' means traffic data and location data and the related data necessary to identify the subscriber or user;

Article 5: categories of data to be retained

1. *Member States shall ensure that the following categories of data are retained under this Directive:*
   - *(a) Data necessary to trace and identify the source of a communication:*
     - *(1) Concerning fixed network telephony and mobile telephony;*
       - *i. The calling telephone number;*
       - *ii. The name and address of the subscriber or registered user;*
     - *(2) Concerning Internet access, Internet e-mail and Internet telephony:*
       - *i. the user ID(s) allocated;*
       - *ii. the user ID and telephone number allocated to any communication entering the public telephone network;*
       - *iii. the name and address of the subscriber or registered user to whom and Internet protocol (IP) address, user ID or telephone number was allocated at the time of the communication;*
   - *(b) Data necessary to identify the destination of a communication:*
     - *(1) Concerning fixed network telephony and mobile telephony:*
       - *i. The number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;*
       - *ii. The name(s) and address(es) of the subscriber(s) or registered user(s);*
     - *(2) Concerning internet e-mail and Internet telephony:*
       - *i. The user ID or telephone number of the intended recipient(s) and user ID of the intended recipient(s) of an Internet telephony call;*
       - *ii. The name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;*
   - *(c) Data necessary to identify the date, time and duration of a communication:*
     - *(1) Concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;*
     - *(2) Concerning Internet access, Internet e-mail and Internet telephony:*

i. The date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) Data necessary to identity the type of communication:

(1) Concerning fixed network telephony and mobile telephony: the telephone service used;

(2) Concerning Internet e-mail and Internet telephony: the Internet service used;

(e) Data necessary to identify users' communication equipment or what purports to be their equipment;

(1) Concerning fixed network telephony, the calling and called telephone numbers;

(2) Concerning mobile telephony:

i. The calling and called telephone numbers;

ii. The International Mobile Subscriber Identity (IMSI) of the calling party;

iii. The International Mobile Equipment Identity (IMEI) of the calling party;

iv. The IMSI of the called party;

v. The IMEI of the called party;

vi. In the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) for which the service was activated;

(3) Concerning Internet access, Internet e-mail and Internet telephony;

(i) The calling telephone number for dial-up access;

(ii) The digital subscriber line (DSL) or other end point of the originator of the communication:

(f) Data necessary to identify the location of mobile communication equipment:

(1) The location label (Cell ID) at the start of the communication;

(2) Data identifying the geographic location of cells by reference to their location labels (Cell iD) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

88. The Joined Cases C-923/12 and C-594/12 ***Digital Rights Ireland and Seitlinger*** challenged the obligation imposed on economic operators to collect and retain, for a specified time, a considerable amount of data generated or processed in connection with electronic communications effected by citizens throughout the territory of the European Union, with the objective of ensuring that such data are available for the purpose of the investigation and prosecution of serious criminal activities and ensuring the proper functioning of the internal market.[18]

89. In the Opinion of Advocate General CRUZ VILLALÓN he stated[19] that the only explicitly excluded data is content and went on to note the large quantities of data that would nevertheless fall within communications data:

> "71. **It is true that Directive 2006/24 excludes from its scope, in a manner which is as express as it is insistent, the content of the telephone or electronic communications, the information communicated itself.**
>
> 72. However, the fact remains that the collection and, above all, the retention, in huge databases, of **the large quantities of data generated or processed in connection with most of the everyday electronic communications of citizens of the Union constitute a serious interference with the privacy of those individuals**, even if they only establish the conditions allowing retrospective scrutiny of their personal and professional activities. The collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitutes a permanent threat throughout the data retention period of the right of citizens of the Union to confidentiality in their private lives. The vague feeling of surveillance created raises very acutely the question of the data retention period.
>
> 73. In that regard, it is first of all necessary to take into account the fact that the effects of that interference are multiplied by the importance acquired in modern societies by electronic means of communication, whether digital mobile networks or the Internet, and their massive and intensive use by a very significant proportion of European citizen in all areas of their private and professional activities."
>
> [emphasis added]

[18] http://curia.europa.eu/juris/document/document.jsf?docid=145562&doclang=EN
[19] http://curia.europa.eu/juris/document/document.jsf?docid=145562&doclang=EN

90. The judgment of the Grand Chamber in *Digital Rights Ireland*, clearly and explicitly referred to the breadth of communications data, as set out in Article 5 of the Data Retention Directive.

91. Emphasising the breadth of communications data, the Court made clear in Digital Rights Ireland, interception and retention on a mass/generalised basis of communications or metadata in itself gives rise to a very serious interference with fundamental rights, irrespective of whether access is subsequently sought or indeed could be subsequently sought. This is because the very fact of retention will affect how individuals communicate, impacting directly on private behaviour.

> *"26. In that regard, it should be observed that the data which providers of publicly available electronic communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data* ***necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services.*** *Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identity the time of the communication as well as the place from which the communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain periods during a given period.*
>
> *27. 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 social environments frequented by them.*
>
> *28. In such circumstances, even though, as is apparent from Article 1(2) and Article 5(2) of the Directive 2006/24, the* ***directive does not permit the retention of the content of the communication*** *or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of*

communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by April 11 of the Charter.

37. It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particular serious. Furthermore, as the Advocate General has pointed out, in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

56. As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, ***the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, internet access, internet e-mail and internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives****…*

57. In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

[emphasis added]

92. As noted by the Advocate General and the Court in *Digital Rights Ireland* a sense of being subject to surveillance has potentially profound implications for individual freedom within the private sphere. What matters is the retention; it is this that potentially affects private behaviour and thus interferences with private life.[20]

[20] The German Constitutional Court referred to this as the "*diffusely threatening feeling of being watched*", see https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html.

93. The consequence of *Digital Rights Ireland* was that the UK's measures implementing the Data Retention Directive were deprived of a legal basis. Accordingly, by way of expedited procedure, the UK Parliament enacted almost identical legislation by way of primary and secondary legislation: the Data Retention And Investigatory Powers Act ("DRIPA") and the Data Retention Regulations 2014 ("the Regulations").

94. DRIPA states that '§2(1) … 'communications data' has the meaning given by section 21(4) of the Regulation of Investigatory Powers Act 2000 ["RIPA"] in so far as that meaning applies in relation to telecommunications services and telecommunications system'[21].

95. RIPA states that :

In this Chapter "communications data" means any of the following—

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—

(i) of any postal service or telecommunications service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

96. The Government accepted, in the national proceedings in *Secretary of State for the Home Department v Tom Watson MP & others* (C-698/15), that the relevant provisions of DRIPA largely duplicated / re-enact the pre-existing UK regime implementing DRD. Indeed, the Government notes in the Bill introducing DRIPA that the *"legislation will mirror the provisions of the existing*

[21] http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf

Data Retention Regulations, and create a clear basis in domestic law for the retention of communications data."[22]

97. The reference to the CJEU in the case of *Secretary of State for the Home Department v Tom Watson MP & others* (C-698/15) concerned data retention powers introduced by the UK following the Court's judgment on 8 April 2014 in the Joined Cases C-923/12 and C-594/12 *Digital Rights Ireland and Seitlinger* (ECLI:EU:C:2014:238) ("DRI"). The questions explicitly concerned the scope of Digital Rights Ireland.

98. Turning to the judgment itself, the CJEU in the Watson judgment explicitly refers to the Digital Rights judgment.

> 98. The data which providers of electronic communications services must therefore retain makes it possible to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to establish the location of mobile communication equipment. That data includes, inter alia, the name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services. That data makes it possible, in particular, to identify the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. Further, that data makes it possible to know how often the subscriber or registered user communicated with certain persons in a given period (**see, by analogy, with respect to Directive 2006/24, the *Digital Rights* judgment, paragraph 26).**
>
> 99. That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, 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 (**see, by analogy, in relation to Directive 2006/24, the *Digital Rights judgment*, paragraph 27**). In particular, that data provides the means, as observed by the Advocate General in points 253, 254 and 257 to 259 of his Opinion, of establishing a profile of the individuals concerned, information that is

22 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/330510/Factsheet_Data_Retention.pdf

no less sensitive, having regard to the right to privacy, than the actual content of communications.

101. Even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights (see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 39), the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter **(see, by analogy, in relation to Directive 2006/24, the *Digital Rights* judgment, paragraph 28)**.

99. These paragraphs in DRI, paragraph 26, 27 and 28 in DRI reference the definition in Article 5 of the Data Retention Directive, and state:

"26. In that regard, it should be observed that the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to **Articles 3 and 5 of Directive 2006/24**, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

27. 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."

28. In such circumstances, even though, as is apparent from Article 1(2) and Article 5(2) of Directive 2006/24, the directive does not permit the

retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter."

100. The CJEU goes on in its judgment to explicitly refers to data relating to subscribers and users and to data stored for billing purpose, which the government seeks to redefine as 'entity' data [see paragraph 84 above].

> "3(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increased capacity for automated storage and processing of **data relating to subscribers and users**."

> "3(26) The **data relating to subscribers** processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. **Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time.** Any further processing of such data … may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing.

101. In its judgment, the CJEU drew no distinction between entity data and any other category of communications data. Nor did the referring court (the Court of Appeal) in the Order for Reference. Nor did the Government suggest at any point during the proceedings, including during the reference, that it was only being asked to consider traffic data and location data.

102. Indeed, in submissions, the Government's representative Daniel Beard QC, only explicitly excluded content, stating that this case was not 'concerned

with the content'. He sought to emphasise the breadth of communications data as a whole stating:

> *"Communications data has been called upon in every major terrorist investigation in the UK in recent years. We have multitudes of examples where communications data has been critical to proving that serious crime has been committed. But it is not just convicting people or identifying accomplices. It can also be used to prove people's innocence. It can confirm an alibi. It can be used to save lives. Calls from those in distress and danger can be identified. Finding kidnap victims, tracking down missing persons, and of course those are not criminal investigations."*

103. In short, the Government made no attempt to assert the position regarding events and entity data it now seeks to do.

104. Instead, as Daniel Beard QC for the UK Government stated in response to questions from the CJEU:

> *"That refers to communications data. That is a definition spelt out in RIPA legislation. You then need to go down to point 15 in this reference, because there is a definition of relevant communications data. It is relevant communications data which can be subject to a retention request under domestic rules. It is that relevant communications data that is defined in section 2(2) of DRIPA. That specifically provides that retained data does not include data revealing the content of a communication."*

> *"To clarify the position that you asked about in relation to scope. In relation to DRIPA there is specific definition of relevant communications data. Communications data of the kind mentioned in the schedule to the 2009 regulations or relevant internet data not falling within paragraph (a) so far as such data is generated or processed in the UK by public telecommunications operators in the process of supplying a telecommunications service concerned. "*

105. The definition of communications data in DRIPA is referred to above. It includes

> (a) *any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;*

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—

(i) of any postal service or telecommunications service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

106. The Data Retention (EC Directive) Regulations 2009 to which Daniel Beard QC refers state:

2(b) Communications data means traffic data, and location data, and the related data necessary to identify the subscriber or user;

107. We are further note the inconsistency and lack of clarity that results from the Government's attempt to exclude types of communications data from the mandatory safeguards as specified in the judgment. For example, the Draft Code of Practice for Communications Data states:

"2.3 Examples of entity date include:
…
Information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes;"

108. However, the 2009 Data Retention Regulations, explicitly referred to by Daniel Beard QC in his submissions on behalf of the UK government, include:

Part 2
Data necessary to identify users' communication equipment (or what purports to be their equipment)
9. (1) The International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI) of the telephone from which a telephone call is made.

(2) the IMSI and IMEI of the telephone dialled
(3) In the case of pre-paid anonymous services, the date and time of the initial activation of the service and the cell ID from which the service was activated.

109. In addition, entity data includes location data which is expressly covered by the CJEU judgment.

110. Further, when looking at the introduction of the Investigatory Powers Act 2016, it is clear the Government were at pains to emphasise that there were very few new powers in the Act and it carried over what was already taking place.

111. According to the Government's own announcements and documentation, what fell under communications data under RIPA, thus under DRIPA, and thus was affected by the judgment in Digital Rights Ireland, as applied by the Watson judgment, did not change under the Investigatory Powers Act, aside from the inclusion of Internet Connection Records.

112. The Communications Data Factsheet for the Investigatory Powers Act 2016 stated:

> *"When necessary and proportionate, CSPs can be required to keep certain types of communications data for up to 12 months under the Data Retention and Investigatory Powers Act 2014 (DRIPA). Law enforcement and the security and intelligence agencies may acquire that data and any other communications data held by CSPs for business purposes under RIPA."*[23]

113. There was a separate Factsheet on 'Internet Connection Records' in line with the announcement of the new category. Then Home Secretary, Theresa May, stated when introducing the Investigatory Powers Bill, that "The draft Bill only proposes to enhance powers in one area – that of communications data retention – and then only because a strong operational case has been made." This referred to Internet Connection Records, which were the only

---

23 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/530550/Communications_Data_factsheet.pdf

type of communications data for which there was stated to be 'no current requirement in law for CSPs to keep'.[24]

114. The Government, in its attempts to distinguish entity data refers to the definitions within the ePrivacy Directive (Directive 2002/58), which the CJEU interpreted in order to arrive at its judgment. This misreads the ePrivacy Directive.

115. Article 1 of the ePrivacy Directive, headed 'Scope and Aim' is clear:

> 1. *This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy,* ***with respect to the processing of personal data in the electronic communication sector*** *and to ensure the free movement of such data and of electronic communication equipment and services in the Community.*[25]

116. Article 4 of the ePrivacy Directive headed 'Services concerned', provides:

> 1. *This Directive shall* ***apply to the processing of personal data*** *in connection with the provision of publicly available electronic communications services in public communications networks in the Community.*[26]

117. The ePrivacy Directive, as stated in its title, applies to *"personal data and the protection of privacy in the electronic communicators sector"* – it applies to communications data, not only select subtypes of data.

118. The ePrivacy Directive was amended by the above referred to Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006. The CJEU's judgment acknowledges and recites Article 1(2) of the Data Retention Directive, which addressed 'Subject matter and scope' as follows:

> *"This Directive* ***shall apply to traffic and location data*** *on both legal entities and natural persons* ***and to the related data necessary to***

---

[24] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/530556/Internet_Connection_Records_factsheet.pdf

[25] Directive 2002/58/EC (the ePrivacy Directive), Article 1(1)

[26] Directive 2002/58/EC (the ePrivacy Directive), Article 3(1)

identity the subscriber or registered user. It shall not apply to the content of electronic communications (…)."[27]

119. The CJEU's judgment confirms the scope of the ePrivacy Directive, which it states at §77 *"must be regarded as regulating the activities of providers of such (*electronic communications) *services"*. The judgment further clarifies that the ePrivacy Directive *"applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies"*. It continues

> *"As confirmed in recital 21 of that directive, the aim of the directive is to prevent unauthorised access to communications, including 'any data related to such communications', in order to protect the confidential electronic communications."*

I. Application of the judgment to business data

120. We are concerned by the Government's statement in the consultation document that:

> "The Government's view is that none of the requirements of the CJEU's judgment relate to the acquisition of data that is being held for business purposes, rather than pursuant to a retention obligation imposed by Government."

121. This suggests that any data held by companies (e.g. for billing purposes) would not be subjected to the safeguards of CJEU for accessing such data.

122. This contradicts the government's own submissions in the case. Daniel Beard QC stated in oral submissions to the CJEU:

> *"we are talking about the retention of data which has to be gathered for commercial reasons and it is to be preserved."*

123. We further note that business data is clearly within the ePrivacy Directive.

124. The Government has failed to elaborate or provide any detail on this position, nor justify it. We submit this 'view' of the requirements of the CJEU judgment is one that if implemented will be found unlawful.

[27] Directive 2006/24/EC (the Data Retention Directive), Article 3(2)

J. Serious crime threshold

125. The Government state in the consultation document that:

> *"Following the CJEU ruling, the Government accepted in the domestic litigation that DRIPA and consequently some aspects of Part 4 of the IPA are inconsistent with EU law, in that:*
> *…*
> *b) **the crime purpose for retaining and accessing data is not limited to serious crime.***
> [emphasis added]

126. The single greatest restraint on powers of access and transmission is the effective limitation of the data retained, as recognised by the Court in DRI.

127. Whilst the Government may accept that aspects of Part 4 are inconsistent with EU law, since the crime purpose for retaining and accessing data is not limited to serious crime, rather than raising the threshold for retaining and access data to serious crime, the Government has simply re-defined 'serious crime'. In doing so it contravenes the finding of the Grand Chamber, that national legislation which provides for general and indiscriminate retention of all traffic and location data; and which precludes the access in the context of fighting crime, is not restricted solely to fighting serious crime.

128. The CJEU emphasised the 'strict' approach to be taken to the objectives which may be relied upon to justify legislation imposing obligations of retention and rights of access to data (see [89]-[90] and [115]). It did so having laid out the powers of retention under s.1 DRIPA and of access under s.22 Regulation of Investigatory Powers Act 2000 at [29] and [32]). It clearly stated that [103]:

> *"given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure."*
>
> See further [105 – 107].

129. The references to serious crime and public security in these passages must be read in light of the CJEU's emphasis at [11] that limited retention and

access powers are only permitted insofar as they fall within the derogation provision in Article 15(1) ePrivacy Directive (see [49], [78], [88], [90] and [115]) and that *'that list of objectives is exhaustive … the Member States cannot adopt such measures for purposes other than those listed in the latter provision"* (at [90]). It necessarily follows that retention and access for purposes other than those purposes is not permitted by EU law.

130. The CJEU gave clear and unequivocal guidance as to the requirement of EU law in relation to access to retained data and serious crime, stating as follows (emphasis added):

> 115. As regards objectives that are capable of justifying national legislation that derogates from the principle of confidentiality of electronic communications, it must be borne in mind that, since, as stated in paragraphs 90 and 102 of this judgment, the list of objectives set out in the first sentence of Article 15(1) of Directive 2002/58 **is exhaustive, access to the retained data must correspond, genuinely and strictly to one of those objectives.** Further, since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, only the **objective of fighting serious crime is capable of justifying such access to the retained data.**
>
> 117. Further, since the legislative measures referred to in Article 15(1) of Directive 2002/58 must, in accordance with recital 11 of that directive, 'be subject to adequate safeguards', a data retention measure must, as follows from the case-law cited in paragraph 109 of this judgment, lay down **clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law.**
>
> 119. Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of

fighting crime, **only to the data of individuals suspected of planning, committing or having a serious crime or of being implicated in one way or another in such a crime…**

131. Previously, as noted in the consultation paper *the general definition of "serious crime" in section 263 of the IPA applies to conduct for which an* ***adult could reasonably be expected to be sentenced to three years or more in prison.*** *(emphasis added).*

132. The definition has been broadened to include offences not traditionally seen as serious crime. As stated in the Draft Communications Data Code of Practice:

> *§3.5 For the purposes of Parts 3 and 4 of the Act "serious crime", defined in section 86(2A) of the Act means: an offence for which an adult is capable of being sentenced to six months or more in prison; any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or a breach of a person's privacy.*

133. In addition to amending the definition of serious crime, the government does not accept that the requirement in the Watson judgment for 'serious crime', applies to all communications data. As stated in the consultation paper, "*The Government proposes to amend the Act to impose a serious crime threshold in relation to the retention and acquisition of* ***events data*** *for criminal purposes".*

> *"The proposed amendments to the legislation provide a definition of 'serious crime' for the purposes of the retention or acquisition of* ***events data,*** *which will apply to investigations into all offences for which an adult is capable of being sentenced to six months or more in prison; any offence involving violence; any offence which involves a large number of people acting in pursuit of a common purpose; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or any offence involving a significant financial gain."*

134. For communications that is not events data, i.e. entity data, or as stated in the Code 'any other case', then the Government will rely on the purpose 'of preventing or detecting crime or preventing disorder' i.e. not serious crime.

135. The Draft Communications Data Code of Practice states:

> *§3.4 The applicable crime purpose will depend on whether the communications data being sought is classified as entity data or events data. The definition of applicable crime purpose is found in section 60A(8) and repeated in sections 61(7A) and 61A(9). It means that where the communications data sought is wholly or partly* ***events data*** *the purpose must be for "serious crime" as defined in section 86(2A). In any other case the communications data must be for the purpose of preventing or detecting crime or preventing disorder.*

136. We submit that the definition of serious crime should at the very least remain as set out in section 263. If there are specific offences the Government would seek to include in the definition of serious crime, these should be explicitly set out. It is the wrong approach to change the definition of serious crime to one that is to all intents and purposes meaningless as it essentially includes all crimes. For example, many minor offences are likely to include sending of a communication, breach of privacy, involve an undefined level of violence.

137. The types of offences which fall under 'serious crime' or 'crime purpose' should be subject to independent review.

138. We disagree with the Government that entity data falls outside the Watson judgment. We therefore submit that all forms of communications data should be subject to the serious crime threshold.

139. Finally, we note that the purpose 'In the interests of public safety' is broad and may also undermine the meaning of 'serious crime'. The Draft Communications Data Code of Practice states:

> *"§3.7 The statutory purpose 'in the interests of public safety' should be used by public authorities with functions to investigate specific and often specialised offences or conduct which as accident investigation or for example, a large-scale event that may cause injury to members of the public."*

K. Statutory purposes for which data can be retained : serious crime

140. Whilst the Government states in the consultation paper that they have removed the three statutory purposes from the IPA: public health; collecting any tax, duty or levy or other imposition, contribution or charge payable to a governmental department; and exercising functions relating to the regulation of financial services and markets or financial stability, this does not apply to Clause 61. This is even though the Government state that:

> *'These three purposes which we propose removing could allow for communications data to be retained or acquired in relation to criminal activity that would not meet the serious crime threshold.'*

141. Clause 61 does not adopt the changes to the 'purposes' subsection, being the purpose for which it is considered 'necessary for the relevant public authority to obtain communications data'. Clause 61 includes, which are not in Clause 60A the following:

> (e) for the purpose of protecting health
> (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,
> (j) for the purpose of exercising functions relating to –
> (i) the regulation of financial services and markets, or
> (ii) financial stability.

L. Access to retained data : independent judicial oversight

142. The CJEU gave clear and unequivocal guidance as to the requirement of EU law in relation to access to retained data, that is must be subject to prior authorisation by independent authority, stating as follows (emphasis added):

> 120. In order to ensure, in practice, that those conditions are fully respected, **it is essential that access of the competent national authorities to retained data** should as a general rule, except in cases of validly established urgency, **be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities,** inter alia, within the framework of procedures for the prevention, detection or prosecution of crime.

143. Despite the above, which clearly requires independent authorisation and oversight for access to communications data, the Government have sought to undermine the judgment in the case of *Secretary of State for the Home Department v Tom Watson MP & others* (C-698/15).

144. The consultation document notes that:

> *"Internal authorisation in other cases*
> *As set out above, the Government's position is that the judgment does not cover requests for communications data made for national security purposes, and we are therefore maintaining the current internal authorisation regime for these cases. Where a pubcli authority may make a request for the purposes of national security or the economic well-being of the UK, where linked to national security (set out in Schedule 4 to the Act), these cases can be authorised by a designated senor officer within the public authority. As now, these designated senior officers will need to be independent of the investigation except in limited circumstances currently defined in the Act.*
>
> *…*
>
> *As set out above, the government considers that entity data is outside the scope of the judgment. However,* ***at present*** *we judge that providing for all communications data applications for entity data to be subject to internal authorisation would make the regime unnecessarily*

complex and under the Government's proposals requests for entity data will be authorised in the same way as request for events data. [emphasis added]

145. We note the Government states 'at present' meaning that this could change. However, we also note as set out below that Schedule 4 allows for entity data to be obtained by those in column 3 for certain purposes.

146. The Data Retention and Acquisition Regulations 2018 provide for the insertion of Clause 60A 'Power of Investigatory Powers Commissioner to grant authorisations'. This provides for circumstances when a public authority must apply to the Investigatory Powers Commissioner in order to be granted authorisation to obtain communications data.

147. However, Clause 61 is maintained. This provides the same power but to be exercised by a designated senior officer - 'Power of a designated senior officer of a relevant public authority' to grant an authorisation to obtain data.

148. The restrictions relating to certain relevant public authorities, i.e. who can apply to a Judicial Commissioner and who can apply to a Designated Senior Officer, is set out in clauses 70, 73, 75 and Schedule 4.

149. According to clause 70:

"(2A) An authorisation under section 60A may be granted on the application of a relevant public authority listed in column 1 of the table only if section 60A(1)(a) is met in relation to a purpose within one of the paragraphs of section 60A(7) specified in the corresponding entry in column 2 of the table.

150. Essentially what is meant is that you look up the public authority in Column 1 of Schedule 4, then look in Column 2 'Paragraphs of section 60A(7) specified' which lists which of the purposes the public authority can rely on. Subsection 60A(7) lists relatively broad purposes. None of those listed for each public authority are surprising and relate to the remit of the public authority listed.

151. What is surprising is the large number of public authorities which can avoid the scrutiny of the Judicial Commissioner and instead seek authorisation to obtain communications data from a Designated Senior Officer.

152. A Designated Senior Officer is:

> *"70(3) In this Part "designated senior officer", in relation to a public authority listed in column 1 of the table, means an individual who holds the authority –*
> *(a) An office, rank or position specified in relation to the authority in column 3 of the table, or*
> *(b) An office, rank or position higher than that specified in relation to the authority in column 3 of the table (subject to subsections (4) and (5)).*"
>
> …
>
> *70(5A) A person who is a designated senior officer of a relevant public authority by virtue of subsection (3) and an entry in column 3 of the table may grant an authorisation under section 61 –*
> *(a) Only for obtaining communications data of the kind specified in the corresponding entry in column 4 of the table,*
> *(b) Only if one or more paragraphs of section 61(7) is specified in the corresponding entry of column 5 of the table, and*
> *(c) Only if section 61(1)(a) is met in relation to a purpose within the specified paragraph or, if more than one paragraph is specified, a purpose within one of them.*
>
> *70(6) A person who is a designated senior officer of a relevant public authority by virtue of subsection (3) and an entry in column 3 of the table may grant an authorisation under section 61A –*
> *(a) Only for obtaining communication data of the kind specified in the corresponding entry in column 4 of the table, and*
> *(b) Only if one or more paragraphs of section 61(7) is specified in the corresponding entry in column 6 of the table, and*
> *(c) Only if section 61(1)(a) is met in relation to a purpose within the specific paragraph or, if more than one paragraph is specified, a purpose within one of them.*

153. What this means, when looking at Schedule 4, is that in non-urgent cases, the following public authorities can obtain communications data, both entity and 'all' types of communications data, (depending on the rank of the DSO), without independent judicial authorisation and oversight, when relying on either purpose (a) 'in the interests of national security' and (c) 'in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security.'

Police force maintained under section 2 of the Police Act 1996; Metropolitan police force; City of London police force; Police Service of Scotland; Police Service of Northern Ireland; British Transport Police; Ministry of Defence; Royal Navy Police; Royal Military Police; Royal Air Force.

154. The Ministry of Defence can only rely on (a) in both urgent and non-urgent cases.

155. In non-urgent cases, the Security Service, Secret Intelligence Service and GCHQ can obtain all types of communications data, for the relevant DSO rank, for (a) and (c) as identified above, and for (b) 'for the applicable crime purpose'.

156. The following do not appear to be able to rely on §61 to obtain communications data i.e. they can't make an application to a DSO in non-urgent cases, but instead must go via the Judicial Commissioner (§60):

Department of Health; Home Office; Ministry of Justice; National Crime Agency; HMRC; Department of Transport; DWP; An ambulance trust in England, Common Services Agency for Scottish Health Service; Competition and Markets Authority; Criminal Cases Review Commissioner; Department for Communities in Northern Ireland; Department for the Economy in Northern Ireland; Department of Justice in Northern Ireland; Financial Conduct Authority; A fire and rescue authority under the Fire and Rescue Services Act 2004; Food Standards Agency; Food Standards Scotland; Gambling Commissioner; Gangmasters and Labour Abuse Authority; Health and Safety Executive; Independent Office for Police Conduct; Information Commissioner; National Health Service Business Services Authority; Northern Ireland ambulance Service Health and Social Care Trust; Northern Ireland Fire and Rescue Service Board; Northern Ireland Health and Social Care Regional Business Services Organisation; Office of Communications; Office of the Police Ombudsman for Northern Ireland; Police Investigations and Review Commissioner; Scottish Ambulance Service Board; Scottish Criminal Cases Review Commission; Serious Fraud Office; Welsh Ambulance Services National Health Service Trust.

157. However, in urgent cases, §61A applies, which extends the types of purposes for those listed under paragraph 26 above to include: (a) ' for the applicable criminal purpose', (b) 'in the interests of public safety', (c) 'for the

purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to person's physical or mental health' and (e) 'where a person ("P") has died or is unable to identify themselves because of a physical or mental condition – (i) to assist in identifying P, or (ii) to obtain information about P's next of kin or other persons concerned with P or about reasons for P's death or condition.

158. This does not include: *Ministry of Defence; Royal Navy Police; Royal Military Police; Royal Air Force* who continue to be able to rely on purposes (a) and (c) not (b) and (e).

159. There are no provisions for the Security Service, Secret Intelligence Service or GCHQ for urgent cases, presumably because the power already exist for non-urgent cases to rely on a DSO, so additional powers are not required for urgent cases.

160. For the remaining public authorities they can rely on applications to DSO's in urgent cases, relying variously on purposes (a), (b), (c), (e).

161. In relation to local authorities, Clause 73 has been amendmended to provide that local authorities can apply for authorisation to obtain communications data to the Judicial Commissioner under §60A.

162. Related to the above, we note our concern with §2.23 – 2.33, specifically data excluded from independent oversight and other safeguards. We are concerned that as stated at §2.33:

> *"Part 3 of the Act does not apply to conduct by a public authority to obtain publicly or commercially available communications data. A communications data authorisation under Part 3 is not mandatory to obtain reference data, such as mobile phone mast locations, from a telecommunications operator as there is no intrusion into an individuals' rights…"*

163. To conclude, under the proposal a significant number of authorities, including the police, immigration authorities and intelligence services will be able to bypass the requirement for independent authorisation.

M. Notification

164. The CJEU gave clear and unequivocal guidance as to the requirement of EU law in relation to notification, stating as follows (emphasis added):

> 121. Likewise, the competent national authorities to whom access to the retained data has been granted **must notify the persons affected,** under the applicable national procedures, **as soon as that notification is no longer liable to jeopardise the investigation** being undertaken by those authorities. **That notification is in fact, necessary to enable the persons affected to exercise, inter alia, their right to legal remedy."**

165. The Government resists implementing this mandatory safeguard and instead refers to the Investigatory Powers tribunal as an avenue of redress. However, the Investigatory Powers Tribunal plays no function if individuals are unaware of the interference with their rights.

166. We note that there are hurdles in place for those seeking redress from the Investigatory Powers Tribunal. In the *Human Rights Watch & Others* case, the Tribunal imposed limits on those whom can seek redress, demonstrating that they were at risk of being subject to certain measures and were present in the UK.[28]

> *"This is a judgment of preliminary issues in respect of the complaints by ten Claimants, including Human Rights Watch ("the Ten"). It arises out of a worldwide campaign by Privacy International. The Tribunal ruled on issues including jurisdiction which will be applied to all remaining campaign related complaints. In respect of any asserted belief that any conduct falling within s.68(5) of RIPA has been carried out by or on behalf of any of the Intelligence Services,* ***a complainant must show that there is a basis for such belief, so that he may show that he is potentially at risk of being subjected to such conduct. Further such a claimant must show in respect of such a complaint that he is or was at a material time present in the United Kingdom.****"*

167. In *Szabo and Vissy v Hungary* the court held:

> "As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned. …

[28] http://www.ipt-uk.com/judgments.asp?id=33

> In Hungarian law, however, no notification, of any kind, of the measures is foreseen. This fact, coupled with the absence of any formal remedies in case of abuses, indicates the legislation falls short of securing adequate safeguards."[29]

168. The Government has chosen to ignore the ruling. Their attitude further appears to treat everyone as suspects. They state in the consultation document that:

> *"A public authority may acquire the data of someone who is a victim of crime to corroborate their claim. Whilst it could be thought appropriate to notify the victim of a crime that their data has been obtained, there are examples where people who were thought to be victims turn out, at a later date, to be involved in the criminality."*

169. It is concerning that victims of crimes, unbeknownst to them, will have their allegations checked via communications data requests, and yet never be told about this.

170. Equally they have failed to give any examples and failed to give statistics on the length of time within which the asserted cases result in a victim turning out be involved in the criminality.

[29] Szabo and Vissy v Hungary, (App No 37138/14 12 January 2016 Fourth Section) paragraph 86

N. Internet Connection Records

171. As has been noted above, the Investigatory Powers Act expands the previous data retention regime under DRIPA to include the retention of 'Internet Connection Records.'

172. Internet Connection Records ("ICRs"), while far from clear in scope, have the potential to intrude significantly into people's private lives. This is combined with a regime of retention of vast quantities of data, which results in the collection and storage, for up to a year, of highly revealing information pertaining to virtually all communications sent, received or otherwise created by us all.

173. The draft Communications Data Code of Practice states:

> *"2.75 There is no single set of data that constitutes an ICR, as it will depend on the service and service provider concerned. The core information that is likely to be included is:*
>
> - *A customer account reference – this may be an account number or an identifier of the customer's device or internet connection;*
> - *The source IP address and port;*
> - *The destination IP address and port – this is the address to which the person is routed on the internet and could be considered as equivalent to a dialled telephone number. The port additionally provides an indication of the type of service (for example website, email server, file sharing service, etc) although ports are often reused for the different purpose; and*
> - *The date/time of the start and end of the event or its duration.*
>
> *2.76 In addition an ICR may also include, for example:*
> *- the volume of data transferred in either, or both, directions;*
> *- the name of the internet service or attributable server that has been connected to;*
> *- those elements of a URL which constitute communications data.*

174. The new version of the Code has deleted (from §2.74 in the new code, previously §2.62) the more explicit statements in the older version that:

> *§2.62 An ICR will only identify the service that a customer has been using.* ***It is not intended to show what a customer has been doing on that service.***

175. The definition of ICR is not technically crafted and the Code merely states what it is 'likely' to include, making it impossible to assess exactly what an ICR would contain and who exactly would be required to retain them. The "Operational Case for the Retention of Internet Connection Records" issued with the draft Investigatory Powers Bill provided a number of scenarios and case studies. This and the draft Communications Data Code of Practice, provide a very conservative view of the capabilities which the Act can authorise.

O. Web browsing

176. The precise definition of an ICR is remains unclear but appears to include the "web logs" addressed by David Anderson QC in his report 'A Question of Trust.'

177. In his report, Anderson noted that "web log" was an uncertain term but quoted the Home Office's 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 records 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."*[30]

178. Anderson concluded that "[u]nder 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."[31]

179. The Draft Communications Data Code of Practice provides detail on 'Web browsing and communications data' at §2.59 - §2.66. The Code later states at §2.68 that relevant communications data includes:

> *"the sender or recipient of a communication (whether or not a person) – this can include … In the context of internet access this can include source and destination IP addresses, port numbers* ***and relevant elements of URLs****;*

[30] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf para 9.53

[31] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf para 9.54

180. In addition to the http protocol (we note that the Code refers to http and does not mention https[32]) and IP address it notes that URL's may contain:

- The port.
- The user info
- The path and optional parameters e.g. 'socialmedia.com/profile/home' the path is profile/home.
- The optional query parameters

181. The Code, in its Autumn 2016 version stated:

> *§2.55 With the exception of the port, and in certain circumstances the userinfo, these elements of a URL, where present, will not constitute communications data."*

182. The new 2017 draft Code states:

> *§2.55 The port and, where required to route a communication, the userinfo will be communications data.*

183. We submit that these changes obfuscate rather than clarify that anything after the first '/' slash in a URL is content. We are concerned in addition as to what is mean by 'relevant elements of URLs' in the context of relevant communications data as referenced above.

184. As we noted in our submissions to the Joint Committee, Anderson expressed deep hesitation about introducing an obligation to retain such data. He noted it had not been demonstrated that "access to weblogs is essential for a wide range of investigations" and that even within the law enforcement community, "it is widely accepted … that the compulsory retention of web logs would be potentially intrusive."[33]

185. Anderson emphasised that any proposal progressing this issue would "need to be carefully thought through and road-tested with law enforcement, legal advisers and CSPs" with robust consultations with "[o]utside technical experts, NGOs and the public".[34] He suggested a detailed list of issues that should be addressed, including, *inter alia:*

---

[32] https://www.digitalgov.gov/2015/03/25/http-vs-https-is-it-time-for-a-change/

[33] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf para 9.60

[34] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf para 14.35

1. The precise definition of the purpose for which such records should be accessible, and the relative importance of those purposes;
2. 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 or by data preservation i.e. an instruction to CSPs to retain web logs or equivalent of a given user who was already of interest to law enforcement;
3. The precise records that would need to be retained for the above purposes and who those records should be defined;
4. The steps that would be needed to ensure the security of the data in the hands of the CSPs;
5. The implications for privacy; or
6. The cost and feasibility of implementing the proposals.[35]

[35] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf para 9.33

P. Technical Capability Notices ("TCN") / Maintenance of Technical Capability

186. TCN's are referred to in the Bulk Acquisition, Equipment Interference and Interception Codes as well as the Communications Data Code. Referring to TCN's across all these creates confusion regarding the full scope of this power. In addition, the definition and obligations required under TCN's is much too vague for the public to adequately foresee the circumstances in which they would be used and the scope of its application.

187. A TCN is 'imposed' on telecommunications operators or postal operators.[36]

188. Undermining Encryption: The Code makes clear that TCN's can be used to undermine encryption.

> *§12.5 … obligations relating to the removal of electronic protection applied by or on behalf of the relevant operator on whom the obligation has been placed, to any communications or data.*

189. These measures would weaken internet security as they would force telecommunications providers to create "backdoors" to encrypted systems, leaving them open to breaches.

> *§12.6 An obligation imposed by a technical capability notice on a telecommunications operator to remove encryption does not require the operator to remove encryption per se. Rather, it requires that operator to maintain the capability to remove encryption when subsequently served with a warrant, notice or authorisation.*

190. This is not simply an obligation on a telecommunications operator to remove encryption, but imposes an obligation to ensure that a person is able to remove electronic encryption.

191. Encryption is essential in the modern world. The stronger it is, the safer we are. The provisions in the Code and in the Draft Investigatory Powers (Technical Capability) Regulations 2017 would enable the Government to order companies like WhatsApp to compromise the security of their products so that the Government can surveil customer data. But digital backdoors can be exploited by criminals and other governments, even if they are designed for Government access.

[36] §12.2 Draft Communications Data Code of Practice

192. Enforcing a TCN should not undermine the confidentiality of communications. We note the Human Rights Council Resolution[37], which states:

> *"Encourages business enterprises to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity,* ***and calls upon States not to interfere with the use of such technical solutions, with any restrictions thereon complying with States' obligations under international human rights law;"***

193. Encryption is an enabler of privacy and freedom of expression, and in turn, keeps individuals safe, by securing their data. Encryption protects individuals most vulnerable to reprisal – from the state, their fellow countrymen or other would-be oppressors – such as journalists, researchers, lawyers and civil society. Thus, in the words of the U.N. High Commissioner for Human Rights:

> *"It is neither fanciful nor an exaggeration to say that without encryption tools, lives may be endangered. In the worse cases, a Government's ability to break into its citizens' phones may lead to the persecution of individuals who are simply exercising their fundamental rights."* [38]

194. Encryption protects ordinary individuals as well. As the U.N. Special Rapporteur for Freedom of Expression has observed, encryption permits all of us to *"search the web, develop ideas and communicate securely."*[39] It also protects all of our data from malicious attackers, such as criminals.

195. Encryption is essential not only for the safety of individuals but also for communications infrastructure. Encryption protects the confidentiality of communications, while providing a way to both authenticate those communications and ensure their integrity. It therefore enables others to assess the legitimacy of the person or institution communicating with them and the legitimacy of the communication itself. This mechanism is essential for banks to protect financial transactions and for business to protect against fraud. For that reason, encryption underpins the secure functionality of the internet and facilitates global online commerce. The digital economy would be impossible without the use of encryption as it ensures that online

[37] A/HRC/34/L/Rev.1 Human Rights Council, Thirty-fourth session, 27 February – 24 March 2017, 'The Right to Privacy in the Digital Age'
[38] OHCHR Press statement, 4 March 2016
[39] UN doc A/HRC/29/32

transactions remain secure and personal data is not captured and exploited. As noted by a leading group of technology experts. *"[it] is impossible to operate the commercial Internet or other widely deployed global communications network with even modest security without the use of encryption."*

196. It is similarly nearly impossible to keep out unauthorised parties from accessing communications while somehow permitting exceptional access only by government officials.[40]

197. The attempt to undermine encryption technologies or limit access to them is often justified by the claim that there should be no place for would-be criminals or terrorists to "hide" – i.e. they should not be able to protect their communications from government surveillance.

198. However, the U.N. Special Rapporteur for Freedom of Expression has noted that while *"[e]ncrypted and anonymous communications may frustrate law enforcement and counter-terrorism officials … State authorities have not generally identified situations … where a restriction has been necessary to achieve a legitimate goal."*

199. He emphasised that *"the public lacks an opportunity to measure whether restrictions on their online security would be justified by any real gains in national security and crime prevention." He also highlighted that such restrictions would have "broad, deleterious effects on the ability of all individuals to exercise freely their rights to privacy and freedom of opinion and expression."*

200. Privacy International strongly recommends that the provisions related to removal are deleted from the Draft Code.

201. Ability to challenge: The subject of a TCN may request review by the Secretary of State. While the Technical Advisory Board and a Judicial Commissioner provide views on the challenge, the Secretary of State makes the decision "to vary, withdraw or confirm the effect of the notice." That decision is then subject to approval by the Investigatory Powers Commissioner.

202. The subject of a TCN should be able to challenge the TCN before an independent authority, preferably a judge. The review of that challenge

[40] Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, Journal of Cybersecurity 2015.

should not be undertaken by the Secretary of State with approval by the IPC.

203. **Interference with business operations:** TCN's will involve significant interference with operations of telecommunications operators. Whether it is to undermine encryption or facilitate interception or equipment interference, these measures would require companies to fundamentally alter their systems, building in permanent capabilities at the behest of the Government, pursuant to the impositions of a TCN.

204. The Draft Investigatory Powers (Technical Capability) Regulations 2017, which would apply to communications data, specified the requirement to "provide, modify, test, develop or maintain" apparatus, systems or other facilities. There were also obligations in relation to reliability and ability to conduct audits.

205. In addition, the Codes and Regulations require telecommunications operators to notify the Secretary of State changes to existing telecommunications services and the development of new services.

> §12.33 Telecommunications operators and postal operators that have been given a technical capability notice may be obliged by regulations to **notify the Secretary of State of changes to existing telecommunications services and the development of new services and relevant products in advance of their launch**. This will enable the Secretary of State to consider whether it is necessary and proportionate to require the telecommunications operator or postal operator to modify an existing capability or provide a new technical capability on the service.

206. The draft Communications Data Code of Practice sets out the 'sorts' i.e. not exhaustive, of obligations that may be included:

- Obligations to provide facilities or services of a specified description;
- Obligations relating to apparatus owned or operated by a relevant operator;
- Obligations relating to the removal of electronic protection applied by or on behalf of the relevant operator on whom the obligation has been placed, to any communications or data;
- …

- Obligations relating to the handling or disclosure of any content or data.

207. These provisions indicate the reach of the government's desire to intrude upon and control business practices. The desire to seamlessly ingest large volumes of data, in real time, from telecommunications operators is evident, particularly when taking into account the provisions in the Regulations which relate to the hand-over interface and near real time hand-over points.

208. We are further concerned about provisions which could ultimately force telecommunications operators to use government developed products, or impact on stifling innovation, especially around privacy and security enhancing technologies. The Draft Communications Data Code of Practice states:

> *§22.21 In certain circumstances it may be more economical for products to be developed centrally, rather than telecommunications operators, postal operators or public authorities creating multiple different systems to achieve the same end. Where multiple different systems exist it can lead to increased complexity, delays and higher costs in updating systems (such as security updates).*
>
> *§22.22 Section 250 of the Act provide a power for a Secretary of State to develop compliance systems. This power could be used for example, to develop consistent systems to be used by telecommunications operators and/or postal operators to retain or disclose communications data or systems to be used by public authorities to acquire communications data. Such systems can operate in respect of multiple powers under the Act.*
>
> *§22.23 Where such systems are developed for use in telecommunications operators and/or postal operators the Secretary of State will work closely with such operators to ensure the systems can be properly integrated into their networks.*

209. We question what the implications would be if a business decided it wished to introduce end-to-end encryption, yet they had to conduct prior consultation with the Secretary of State regarding this, which would undermine the desire of the Secretary of State for backdoor access.

210. The Code must provide greater transparency as to the types of dedicated and compliance systems that may be required under TCNs. It should also

prohibit the requirement that companies adopt such systems where it would compromise the security and integrity of the company's existing systems. The Code must further narrow the circumstances and the scope to which companies must notify the government of changes to existing services or the development of new ones to those strictly relevant to the TCN.

211. Finally, we are concerned that the involvement of the Judicial Commissioner does not appear to relate to technical oversight. The involvement appears to be limited to reviewing the Secretary of State's conclusions as to whether the notice is necessary and whether the conduct it requires is proportionate to what is sought to be achieved.

212. Given the IPCO have stated publicly they will have technical expertise, we submit that it is vital that the IPCO can conduct in-depth independent review of the technical aspects of TCN's, the impact on systems and on security.

Q. Additional concerns

213. The Draft code of practice for Communications Data contains a large number of provisions that are of concern. If we have not mentioned an aspect of the Code, that does not imply that we agree with the provisions. However, due to the short time to respond and very lengthy document, we briefly note the following.

214. Systems data. The Code refers to systems data and states that systems data is by definition not content (§2.15 – 2.17). We raised in our submissions to the previous consultation on the other Codes of Practice under the Investigatory Powers Act our concerns that the Codes allow content to be redefined as systems data [see paragraphs 2.17 – 2.31]

215. Necessity and Proportionality: we refer to our submissions in relation to the other Codes of Practice under the Investigatory Powers Act in §10 which are relevant to the Communications Data Code.

216. Third Party data: The draft Communications Data Code refers at §2.80 -2.83 to third party data. It has removed §2.70 from the old Code which stated:

> *"A retention notice cannot require a CSP to retain third party data. Accordingly an ICR retained by a CSP may only include data that the*

CSP itself needs to transmit the communications, unless the CSP retains additional relevant data about the third party service for their own business purposes."

217. **Less intrusive means:** The draft Communications Data Code of Practice (§3.16, 3.24, 9.15, 12.14, 16.2, 17.19) , and relevant aspects of the Act, refer to 'less intrusive means'.

218. Whilst this is in theory a positive statement, it is meaningless without an analysis or explanation as to what constitutes 'less intrusive means', how a determination of intrusiveness is conducted, who conducts the assessment and what oversight exists to scrutinise whether less intrusive in theory is less intrusive in practice.

219. **Novel or contentious acquisition:** as identified at §8.46 – 8.55, this should involve the IPCO and not just the SPoC.

220. **The request filter:** This is set out at paragraph 11 in the Draft Communications Data Code of Practice. We have repeatedly noted our concerns with the Request Filter and the lack of clarity around this and how it will operate.

R. Security issues

221. We note with concern § 2.41 of the draft Communications Data Code of Practice, which states:

"Some telecommunications operator may choose to retain user passwords as clear text for business purposes. In this context passwords would constitute entity data."

222. We are concerned that whilst the Code acknowledges that data retention and disclosure systems must be compliant with relevant data protection legislation, the Code fails to make any clear statement in relation to the potential breach of Data Protection Principle 7 under the Data Protection Act 1998 to be replaced by the integrity and confidentiality principle under the EU General Data Protection Regulation (GDPR), and the clear risks of businesses storing passwords in clear text.

223. It is equally concerning that these are treated as entity data and thus not subject to judicial oversight. It is worrying that public authorities could be

storing clear text passwords they have obtained using communications data powers.

S. Data Protection

224. The Code of Practice mentions adherence with relevant data protection legislation, however it fails to provide clear guidance on the interaction between the Investigatory Powers Act, the Regulations, the Code of Practice and such data protection legislation. For example, in relation to 'Excess Data' the Code fails to explain the purpose limitation principle in the Data Protection Act 1998 and included in the forthcoming GDPR and Law Enforcement Directive which will be implemented by the Data Protection Bill currently progressing through Parliament. Otherwise data protection is only mentioned at a very general level in terms of data security and integrity and in terms of transfers of data outside the EU.

225. Data protection is a fundamental human right, enshrined by Article 8 of the European Convention on Human Rights, Articles 7 and 8 of the European Charter of Fundamental Rights as well as various instruments of International Human Rights Law and national and European legislation (the Data Protection Act 1998 to be replaced with the GDPR and the Data Protection Act (2018)). Therefore, it is essential that the Communications Data Code of Practice which covers the handling of mass amounts of personal data provides clear, informative and accurate guidance on the interaction between the exercise of functions conferred under the Investigatory Powers Act covered by the Code and the requirements on telecommunications operators, postal operators and public authorities to comply with data protection legislation.