ARRANGEMENTS FOR THE ACQUISITION OF BULK COMMUNICATIONS DATA PURSUANT TO DIRECTIONS UNDER SECTION 94 OF THE TELECOMMUNICATIONS ACT 1984

Contents

1.0	Introduction	p.1
2.0	What information these Arrangements cover	p.1
3.0	The law	p.2
4.0	Safeguards and Oversight	p.4
4.1	Authorisations	p.4
4.2	Acquisition	p.5
4.3	Use and Access	p.5
4.4	Disclosure	p.7
4.5	Review of Ongoing Acquisition/Retention and Deletion	p.8
4.6	Oversight	p.9

1.0 Introduction

1.1 These Handling Arrangements are made under section 2(2)(a) of the Security Service Act 1989 ("the **SSA 1989**") and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 ("**the ISA 1994**") ("**the information gateway provisions**"). They come into force on 4th November 2015.

1.2 The Arrangements apply to the Security Service (MI5), the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ), hereafter 'the Intelligence Services', with respect to their acquisition of bulk communications data ("BCD") under section 94 of the Telecommunications Act 1984 and the subsequent use and disclosure of such data.

1.3 The rules set out in these Arrangements are mandatory and are required to be followed by staff in the relevant Intelligence Services. References in these Arrangements to 'staff' are to staff in these Services unless specified otherwise. Failure by staff to comply with these Arrangements may lead to disciplinary action, which can include dismissal and prosecution.

2.0 The information covered by these Arrangements

2.1 The Intelligence Services need to collect a range of information from a variety of sources to meet the requirements of their statutory functions, and do this in accordance with the information gateway provisions.

2.2 Among the range of information collected is communications data under Section 94 of the Telecommunications Act. The communications data collected is limited to "**Traffic Data**" and "**Service Use Information**" [*see paragraph 3.5.1 and 3.5.2 below for definitions of "Traffic Data" and "Service Use Information"*].

2.3 The data provided does not contain communication content or Subscriber Information [*see paragraph 3.5.1 below for definition of "Subscriber Information"*], nor does it include 'Internet Connection Records'.

2.4 Any section 94 Directions under which this communications data is acquired requires the relevant Secretary of State to be satisfied that acquisition is necessary in the interests of national security or international relations and that the level of interference with privacy involved in doing so is proportionate to what it seeks to achieve.

3.0 The law

3.1 The SSA 1989, the ISA 1994 and the Counter-Terrorism Act 2008 ("the CTA")

3.1.1 The SSA 1989 provides that the functions of the Security Service are the protection of national security, the safeguarding of the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands and the provision of support to the police and other law enforcement authorities in the prevention and detection of serious crime.

[redacted]

Rights. In practice, this means that any interference with privacy must be both necessary for the performance of a statutory function of the relevant Intelligence Service and proportionate to the achievement of that objective.

3.3 The Data Protection Act 1998 ("the DPA")

3.3.1 Each of the Intelligence Services is a data controller in relation to all the personal data that it holds. Accordingly, when the Intelligence Services use any bulk data that contain personal data, they must ensure that they comply with the DPA (subject only to cases where exemption under section 28 is required for the purpose of safeguarding national security).

3.4 Telecommunications Act 1984

3.4.1 **Section 94** of the **Telecommunications Act 1984** (as amended by the Communications Act 2003) – 'the Telecommunications Act' - provides that the Secretary of State may give to providers of public electronic communications networks ("**CNPs**") "*such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom.*" The Secretary of State shall not give a direction unless he believes that the conduct required by the

[redacted]

4.0.1 The acquisition, use, retention and disclosure of BCD requires clear justification, accompanied by detailed and comprehensive safeguards against misuse and must be subject to rigorous oversight.

4.0.2 These Arrangements accordingly provide specific published guidance to staff in the Intelligence Services with respect to the obtaining of BCD under section 94 of the Telecommunications Act and its subsequent use, retention, disclosure and deletion. Staff must ensure that no BCD from this source is obtained, used, retained or disclosed **except in accordance with the information gateway provisions, section 94 of the Telecommunications Act and these Arrangements.**

4.1 Authorisation

4.1.1 Where the head of the relevant Intelligence Service has decided to request a Section 94 Direction from the relevant Secretary of State, it is essential that a submission is then presented to the Secretary of State by the Home Office/Foreign Office in order to enable them to consider:

- whether acquisition and retention of the BCD to be authorised by the Direction is necessary in the interests of national security or international relations;
- whether the acquisition and retention of the BCD would be proportionate to what is sought to be achieved;
- whether there is a less intrusive method of obtaining the BCD or achieving the national security objective;
- the level of collateral intrusion caused by acquiring and utilising the requested BCD.

4.1.2 The submission must also outline any national security or international relations argument as to why the Secretary of State cannot lay the Direction before each House of Parliament in accordance with 94(4) of the Act.

When will acquisition be "necessary"?

4.1.3 What is **necessary** in a particular case is ultimately a question of fact and judgement, taking all the relevant circumstances into account. In order to meet the '**necessity**' requirement in relation to acquisition and retention, before presenting the submission referred to in paragraph 4.1.1 above, staff in the relevant Intelligence Service must consider why obtaining the BCD in question is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service. In practice this means identifying the intelligence aim which is likely to be met and giving careful consideration as to how the data could be used to support achievement of that aim.

The obtaining must also be "proportionate"

4.1.4 The obtaining and retention of the bulk communications dataset must also be **proportionate** to the purpose in question. In order to meet the '**proportionality**' requirement, before presenting the submission referred to in paragraph 4.1.1 above, staff in the relevant Intelligence Service must balance (a) the level of interference with the right to privacy of individuals whose communications data is being obtained (albeit that at the point of initial acquisition of the BCD the identity of the individuals will be unknown), both in relation to subjects of intelligence interest and in relation to other individuals who may be of no intelligence interest, against (b) the expected value of the intelligence to be derived from the data. Staff must be satisfied that the level of interference with the individual's right to privacy is justified by the value of the intelligence that is sought to be derived from the data and the importance of the objective to be achieved. Staff must also consider whether there is a reasonable

alternative that will still meet the proposed objective - i.e. which involves less intrusion.

When seeking authorisation of a new set of BCD, the Intelligence Service must consider and articulate the following for the Secretary of State to consider:

- **The reasons why is it necessary to acquire and retain the data.**
- **The proportionality of acquiring and retaining the data. In particular, whether there is a less intrusive method of obtaining the data or intelligence dividend.**
- **The level of collateral intrusion in acquiring and utilising the proposed data.**

4.2 Acquisition

4.2.1 Should the Secretary of State agree to give the Direction, it will be served on the CNP concerned in order to enable the relevant Intelligence Service to receive the requested dataset.

4.2.2 It is essential that any BCD is acquired in a safe and secure manner and that Intelligence Services safeguard against unauthorised access. Intelligence Services must therefore adhere to the controls outlined in the CESG[1] Good Practice Guide for transferring and storage of data electronically or physically.

4.3 Use and Access

4.3.1 Each Intelligence Service must attach the highest priority to maintaining data security and protective security standards. Moreover, each Intelligence Service must establish handling procedures so as to ensure that the integrity and confidentiality of the information in BCD held is fully protected, and that there are adequate safeguards in place to minimise the risk of any misuse of such data and, in the event that such misuse occurs, to ensure that appropriate disciplinary action is taken.

4.3.2 In particular, each Intelligence Service must apply the following protective security measures:

- Physical security to protect any premises where the information may be accessed;
- IT security to minimise the risk of unauthorised access to IT systems;
- A security vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

4.3.3 Furthermore, each Intelligence Service is obliged to put in place the following additional measures:

- Access to BCD must be strictly limited to those with an appropriate business requirement to use these data and managed by a strict authorisation process;

[1] UK Government's National Technical Authority for Information Assurance.

- Requests to access BCD must be justified on the grounds of **necessity** and **proportionality** and must demonstrate consideration of collateral intrusion and the use of any other less intrusive means of achieving the desired intelligence dividend.
- Intelligence Service staff who apply to access BCD must have regard to the further guidance on the application of the **necessity** and **proportionality** tests set out in paragraph 4.1.3 - 4.1.4 above.
- Where Intelligence Service staff intend to access BCD relating to the communications of an individual known to be a member of a profession that handles privileged information or information that is otherwise confidential (medical doctors, lawyers, journalists, Members of Parliament, Ministers of religion), they must give **special consideration** to the necessity and proportionality justification for the interference with privacy that will be involved;
- In addition, Intelligence Service staff must take particular care when deciding whether to seek access to BCD and must consider whether there might be unintended consequences of such access to BCD and whether the public interest is best served by seeking such access;
- In all cases where Intelligence Service staff intentionally seek to access and retain BCD relating to the communications of individuals known to be members of the professions referred to above, they must record the fact that such communications data has been accessed and retained and must flag this to the Interception of Communications Commissioner at the next inspection;
- In the exceptional event that Intelligence Service staff were to seek access to BCD specifically in order to determine a journalist's source, they should only do this if the proposal had been approved beforehand at Director level. Any communications data obtained and retained as a result of such access must be reported to the Interception of Communications Commissioner at the next inspection;
- Users must be trained on their professional and legal responsibilities, and refresher training and/or updated guidance must be provided when systems or policies are updated;
- A range of audit functions must be put in place: users should be made aware that their access to BCD will be monitored and that they must always be able to justify their activity on the systems;
- Appropriate disciplinary action will be taken in the event of inappropriate behaviour being identified;
- Users must be warned, through the use of internal procedures and guidance, about the consequences of any unjustified access to data, which can include dismissal and prosecution.
- In the exceptional event that Intelligence Service staff were to abuse their access to BCD – for example, by seeking to access the communications data of an individual without a valid business need – the relevant Intelligence Service must report the incident to the Interception of Communications Commissioner at the next inspection.

Intelligence Services must have the following controls on use and access to BCD:

- **Appropriate physical security for premises, IT security for IT systems**

and vetting regime for staff.

- Limit access to those with appropriate business requirement.
- Justify access to BCD on the grounds of necessity and proportionality, taking into consideration collateral intrusion and other less intrusive methods of deriving the same intelligence dividend.
- Ensure staff are appropriately trained, aware of audit functions and warned of disciplinary procedures resulting from misuse.

4.4 Disclosure

4.4.1 The disclosure of BCD must be carefully managed to ensure that it only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The disclosure of an entire bulk communications dataset, or a subset, outside the Intelligence Service may only be authorised by a Senior Official[2] or the Secretary of State.

4.4.2 Disclosure of individual items of BCD outside the relevant Intelligence Service may only be made if the following conditions are met:

- that the objective of the disclosure falls within the Service's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;
- that it is **necessary** to disclose the information in question in order to achieve that objective;
- that the disclosure is **proportionate** to the objective;
- that only as much of the information will be disclosed as is **necessary** to achieve that objective.

When will disclosure be necessary?

4.4.3 In order to meet the '**necessity**' requirement in relation to disclosure, staff in the relevant Intelligence Service and (as the case may be) the Secretary of State must be satisfied that disclosure of the BCD is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service.

The disclosure must also be "proportionate"

4.4.4 The disclosure of the BCD must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff in the relevant Intelligence Service and (as the case may be) the Secretary of State must be satisfied that the level of interference with the right to privacy of individuals whose communications data is being disclosed, both in relation to subjects of intelligence interest and in relation to other individuals who may be of no intelligence interest, is justified by the benefit to the discharge of the Intelligence Service's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of

[2] Equivalent to a member of the Senior Civil Service.

communications data or of a subset of the bulk communications data rather than of the whole bulk communications dataset.

4.4.5 Before disclosing any BCD, staff must take reasonable steps to ensure that the intended recipient organisation has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data and ensuring that it is securely handled, or that they have received satisfactory assurances from the intended recipient organisation with respect to such arrangements.

4.4.6 These conditions must be met for all disclosure, including between the Intelligence Services and apply equally in making the decision to disclose an entire BCD, a subset of BCD, or an individual piece of data from the dataset.

Disclosure of BCD must be:

- **Justified on the basis of the relevant statutory disclosure gateway;**
- **Assessed to be necessary and proportionate to the objective;**
- **Limited to only as much information as will achieve the objective;**
- **Authorised by a Senior Official or Secretary of State (entire BCD or a subset).**

4.5 Review of Ongoing Acquisition and Retention, and Deletion

4.5.1 Each Intelligence Service must regularly review, i.e. at intervals of no less than six months, the operational and legal justification for its continued retention and use of BCD. This should be managed through a review panel comprised of senior representatives from Information Governance/Compliance, Operational and Legal teams.

4.5.2 The retention and review process requires consideration of:

- An assessment of the value and use of the dataset during the period under review and in a historical context;
- the operational and legal justification for ongoing acquisition, continued retention, including its necessity and proportionality;
- The extent of use and specific examples to illustrate the benefits;
- The level of actual and collateral intrusion posed by retention and exploitation;
- The extent of corporate, legal, reputational or political risk;
- Whether such information could be acquired elsewhere through less intrusive means.

4.5.3 Should the review process find that there remains an ongoing case for acquiring and retaining BCD, a formal review will be submitted at intervals of no less than six months for consideration by the relevant Secretary of State. In the event that the Intelligence Service or Secretary of State no longer deem it to be necessary and proportionate to acquire and retain the BCD, the Secretary of State will cancel the relevant Section 94 Direction and instruct the CNP concerned to cease supply. The relevant Intelligence Service must then task the technical team[s] responsible for Retention and Deletion with a view to ensuring that any retained data is destroyed and notify the Interception of Communications Commissioner accordingly. Confirmation of completed deletion must be recorded with the relevant Information Governance/Compliance team.

For the purposes of retention, review and deletion of BCD holdings, Intelligence Services must:

- **Review holdings on a regular six-monthly basis to ensure that ongoing acquisition, retention and use remains necessary and proportionate to carry out their statutory functions;**
- **Submit every six months a copy of the review for consideration by the Secretary of State;**
- **Delete BCD holdings after any decision is made that it is no longer necessary or proportionate to hold the data and notify the Interception of Communications Commissioner accordingly.**

4.6 Oversight

Internal

4.6.1 The acquisition, retention and disclosure of BCD is subject to scrutiny in each Intelligence Service by the internal review panel (outlined in paragraph 4.5.1). A senior member of this review panel must keep the Executive Board apprised of BCD holdings.

4.6.2 Use of IT systems is monitored by the audit team in order to detect misuse or identify activity that may give rise to security concerns. Any such identified activity initiates a formal investigation process in which legal, policy and HR (Human Resources) input will be requested where appropriate. Disciplinary action may be taken, which in the most serious cases could lead to dismissal and/or the possibility of prosecution under the Computer Misuse Act 1990, the Data Protection Act 1998, the Official Secrets Act 1989 and Misfeasance in Public Office depending on circumstances.

4.6.3 All reports on audit investigations are made available to the Interception of Communications Commissioner (see paragraph 4.6.4 - 4.6.8 below).

External

4.6.4 The **Interception of Communications Commissioner** has oversight of:

a) the issue of Section 94 Directions by the Secretary of State enabling the Intelligence Services to acquire BCD;

b) the Intelligence Services' arrangements in respect of acquisition, storage, access, disclosure, retention and destruction; and

c) the management controls and safeguards against misuse which the Intelligence Services have put in place.

4.6.5 This oversight is exercised by the Interception of Communications Commissioner on at least an annual basis, or as may be otherwise agreed between the Commissioner and the relevant Intelligence Service.

4.6.6 The purpose of this oversight is to review and test judgements made by the Secretary of State and the Intelligence Services on the necessity and proportionality of the Section 94 Directions and on the Intelligence Services' acquisition and use of

BCD, and to ensure that the Intelligence Services' policies and procedures for the control of, and access to BCD are (a) are sound and provide adequate safeguards against misuse and (b) are strictly observed.

4.6.7 The Interception of Communications Commissioner also has oversight of controls to prevent and detect misuse of data acquired under Section 94, as outlined in paragraph 4.6.2 and 4.6.3 above.

4.6.8 The Secretary of State and the Intelligence Services must provide to the Interception of Communications Commissioner all such documents and information as he may require for the purpose of enabling him to exercise the oversight described in paragraph 4.6.4 - 4.6.7 above.

Oversight of BCD holdings must include:

- **Internal review panel reports to the Executive Board on BCD holdings;**
- **Internal audit of systems to detect misuse or identify activity of security concern with corresponding disciplinary measures; and**
- **External, independent oversight by the Interception of Communications Commissioner of the acquisition, retention and disclosure of and access to BCD holdings on an annual basis.**

Published: 4th November 2015