This information has been gisted.

GCHQ Section 94 Closed Handling Arrangements

1. Introduction

1.1 These Handling Arrangements are made under section 4(2)(a) of the Intelligence Services Act 1994 ("ISA"). They come into force on 4 November 2015.

1.2 The Arrangements apply to the Government Communications Headquarters (GCHQ) with respect to its acquisition of bulk communications data pursuant to directions given by the Secretary of State under section 94 of the Telecommunications Act 1984 ("section 94 data"), and to its subsequent use and disclosure of such data. In brief, section 94 data is to be handled in the same way as related communications data obtained pursuant to warrants issued by the Secretary of State under section 5 of the Regulation of Investigatory Powers Act 2000 ("RIPA").

1.3 The rules set out in these Arrangements are mandatory and are required to be followed by staff in GCHQ. References in these Arrangements to 'staff' are to all persons working for or at (but not on behalf of) GCHQ unless specified otherwise. Failure by staff to comply with these Arrangements may lead to disciplinary action, which can include dismissal, and potentially to criminal prosecution.

1.4 Since 2001 successive Foreign Secretaries have given directions, under section 94 of the Telecommunications Act 1984 ("the section 94 directions"), requiring a number of providers of public electronic communications networks ("CNPs") to provide GCHQ with various sets of bulk communications data in the interests of national security. All the sets of communications data currently being provided have a foreign focus insofar as one or both ends of each communication will be located overseas and/or one or both communication devices will be foreign-registered. GCHQ provides a review of the use of this communications data, and of the continuing need to acquire it (where this can be justified), to the Foreign Secretary at six-monthly intervals.

2. The information covered by these Arrangements

2.1 The communications data provided by the CNPs under the section 94 directions is limited to various forms of "traffic data" (as defined in section 21(6) RIPA) and "service use information" (as defined in section 21(4)(b) RIPA).

2.2 The data provided does not contain communications content or "subscriber information" (as defined in section 21(4)(c) RIPA), nor does it include "Internet Connection Records".

First stage: acquisition of section 94 data

2.3 The processing of section 94 data involves two distinct stages. The first is acquisition, the point at which – pursuant to the section 94 directions referred to in paragraph 1.4 above – the CNPs each transfer their data to GCHQ for secure retention in operational systems accredited to hold bulk communications data.

2.4 The section 94 directions under which this transfer takes place require the Foreign Secretary to be satisfied that the supply of data is necessary in the interests of national security and that the conduct required by the direction – including any interference with privacy – is proportionate to what it seeks to achieve.

Second stage: use of section 94 data

2.5 The second stage involves the use of section 94 data by trained GCHQ analysts, normally by running queries against the appropriate operational systems. These systems are also likely to contain related communications data derived from interception conducted in accordance with section 8(4) RIPA warrants.

[REDACTED]

2.7 Data may only be queried and viewed by analysts if the conduct involved is in accordance with GCHQ's statutory functions and purposes and is considered necessary and proportionate. Individual analysts are required to provide a statement of necessity and proportionality ("N&P statement") for any analytical search of a system containing section 94 data or related communications data. (See paragraph 4.3.5 for a fuller explanation of N&P statements.) N&P statements may be audited.

[REDACTED]

3. The law

3.1 General information on the main laws affecting GCHQ's operations, including ISA and RIPA, may be found in the "Overview" and "Laws" sections of GCHQ's Compliance Guide.

Telecommunications Act 1984

3.2 Section 94 of the Telecommunications Act 1984 (as amended by the Communications Act 2003) provides that the Secretary of State may give to 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 direction is "*proportionate to what is sought to be achieved by that conduct*". The Secretary of State is also required to consult a CNP before he gives a direction relating to it.

3.3 As indicated in paragraph 1.4 above, successive Foreign Secretaries have given section 94 directions in respect of a number of CNPs. Since 2013 GCHQ has provided a review of these directions to the Foreign Secretary every six months.

3.4 Section 94(4) provides that the Secretary of State must lay a copy of every direction before each House of Parliament "*unless he is of the opinion that disclosure of the direction is against the interests of national security*". The Foreign Secretary is of the view that disclosure of the section 94 directions given on the application of GCHQ would be against the interests of national security, and so these directions have not been published, nor has the fact of their existence with respect to particular CNPs.

Counter-Terrorism Act 2008

3.5 Section 19 of the Counter-Terrorism Act 2008 confirms that information obtained by GCHQ in connection with the exercise of any of its functions may be used by GCHQ in connection with the exercise of any of its other functions. On this basis, information obtained by GCHQ under section 94 directions for national security purposes may subsequently be used by GCHQ in the interests of the economic well-being of the UK and to support the prevention or detection of serious crime.

4. Safeguards and Oversight

4.0.1 The acquisition, use, retention and disclosure of section 94 data 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 GCHQ with respect to the acquisition of section 94 data, access to and use of the data, retention of the data, and disclosure of the data to persons outside GCHQ where this is necessary for the proper discharge of GCHQ's statutory functions. Staff must ensure that no section 94 data is accessed, used, retained or disclosed except in accordance with section 4(2)(a) of ISA, section 94 of the Telecommunications Act 1984 and these Arrangements.

4.1 Authorisation of Acquisition – Stage 1

4.1.1 Where *the relevant senior GCHQ official* has agreed to request a section 94 direction from the Foreign Secretary, a submission will be drafted by *the relevant team* in order to enable the Secretary of State to consider:

- whether the direction is necessary in the interests of national security or relations with the government of a country or territory outside the UK;
- whether the conduct required by the direction is proportionate to what is sought to be achieved by that conduct;
- whether there is a less intrusive means of achieving the national security objective(s) of the direction;
- any political and reputational risks in directing the CNP to provide the specified communications data.

4.1.2 This submission will be informed by extensive preparatory work by GCHQ in order to consider and articulate the necessity and proportionality of acquiring, retaining and using the communications data to be requested under the direction. GCHQ will also consult the CNP concerned on behalf of the Secretary of State and the submission will reflect the views of the CNP as part of the overall consideration.

4.1.3 The submission must be endorsed by a GCHQ Legal Adviser, to confirm that all legal criteria for requesting a section 94 direction have been satisfied.

4.1.4 The submission must also outline any national security argument as to why the Foreign Secretary cannot lay the direction before each House of Parliament in accordance with section 94(4) of the Act.

4.2 Acquisition

4.2.1 *Should the Foreign Secretary agree to give the direction, it will be served on the relevant CNP.*

[REDACTED]

4.3 Authorisation of Use/Access – Stage 2

4.3.1 Access to section 94 data on operational systems is controlled through standard GCHQ account management procedures, which ensure that system access is granted only to those with a genuine, operational requirement to access the data. Within systems, access to specific, particularly sensitive, data can be further limited through electronic access control measures such as "Communities of Interest" and "Access Control Groups". **[REDACTED]** Systems holding section 94 data are also likely to contain related communications data derived from interception conducted in accordance with section 8(4) RIPA warrants.

[REDACTED]

4.3.3 Individuals must also sign up to the *appropriate operating procedures*. These make clear that access to operational systems is granted, and must be used, only for legitimate, work-related purposes. Records of individuals' access to, and use of, GCHQ IT systems are centrally logged and regularly monitored for evidence of abuse.

4.3.4 In the case of systems containing operational data, such as section 94 data, specific details of individuals' activities while accessing the system are logged and are subject to audit. Such logs contain details of who was accessing the system, when, and what they did while logged in.

4.3.5 Any analytical search or query with respect to an operational system containing section 94 data or related communications data must be necessary and proportionate. Before conducting any such search or query, individual analysts must provide a justification in the form of an N&P statement. An N&P statement consists of a record of the operational purpose of the search or query and a free-text explanation of its necessity and proportionality.

4.3.6 In this context, "necessary" means "really needed" for the purpose of discharging one or more of GCHQ's statutory functions.

4.3.7 In deciding whether a search or query is necessary, analysts must consider:

- The background and aims of the intelligence operation in question.
- Where the query relates to a known target, what is the significance of the target in the context of the intelligence operation?
- How does the communications address that is the subject of the query relate to the target and/or to the intelligence operation?
- How will the data to be retrieved assist in taking forward the intelligence operation?

4.3.8 In this context, "proportionate" means that the level of interference with the individual's right to privacy is justified when measured against the anticipated intelligence benefit and the importance of the objective to be achieved.

4.3.9 In deciding whether a search or query is proportionate, analysts must consider:

- What exactly is being sought in the data to be retrieved?
- What will be the intrusion into the privacy of the target of the query? Can this be justified by the intelligence benefits?
- Is there another, less intrusive way of obtaining the information required?
- If a time period of data has been specified, why is this particular time period required? Would a shorter time period be sufficient?

4.3.10 Any collateral intrusion must be considered as part of proportionality. In particular, analysts must consider:

- Will the data to be retrieved result in collateral intrusion into the privacy of persons unconnected with the aims of the intelligence operation? Can this be justified by the intelligence benefits?
- If a time period of data has been specified, how will this impact on the identified collateral intrusion?
- How will any identified collateral intrusion be managed? For example, if seeking to retrieve call records data for a landline used by individuals of no intelligence interest as well as the target, how will the data be analysed to identify usage by the target?

4.3.11 Analysts must give special consideration to any search or query that is likely to retrieve communications data relating to a member of a profession that handles privileged information or information that is otherwise confidential (i.e. lawyers, journalists, medical professionals, ministers of religion or UK Members of Parliament). This consideration should be recorded in the N&P statement.

4.3.12 In any case where analysts include information based on communications data relating to individuals known to be members of the professions referred to above within *intelligence reporting*, this must be recorded and brought to the attention of the Interception of Communications Commissioner at the next inspection.

4.3.13 In any exceptional case where analysts wish to access communications data in order to determine a journalist's source, they should seek approval to do so from *the relevant GCHQ senior official*. Any such information that is included in an *intelligence report* must be brought to the attention of the Interception of Communications Commissioner at the next inspection.

[REDACTED]

4.4 Authorisation of Disclosure

4.4.1 Where the results of analysing section 94 data are disclosed to partner or customer organisations, this must be done via standard *intelligence* reporting mechanisms, which ensure that GCHQ intelligence is released in a secure, accountable and legally compliant manner.

4.4.2 If disclosure of a complete section 94 dataset, or a substantial part of it, to a partner organisation is contemplated, whether at GCHQ's or the partner's initiative, the procedures below must be followed.

4.4.3 If the proposed recipient of the dataset is another SIA Agency, that Agency will (as with any other operational data) formally request transfer of the data via the "Inter-Agency Sharing" (IAS) process. As with authorisation to acquire section 94 data, this disclosure request will be considered and authorised (or rejected) by *the relevant GCHQ senior officials*. The Authoriser's decision and the reasons for it will be recorded on the IAS form.

4.4.6 All requests for authorisation to disclose must provide a persuasive justification for the proposed disclosure, in terms of:

- its necessity and proportionality, and
- the intelligence benefit or other operational benefit that is expected to accrue to GCHQ and the UK from the disclosure.

4.4.7 The Authoriser will consider:

- the content of the dataset: the nature of any personal information it contains, its intrusiveness and sensitivity;
- the nature and extent of the corporate risk the disclosure would entail;
- the necessity and proportionality of the disclosure, including whether it is genuinely necessary and proportionate to disclose the whole dataset, or whether a subset will meet the need;
- whether any caveats or restrictions should be applied; and
- the receiving organisation's arrangements for safeguarding, using and deleting the data – GCHQ will seek additional reassurances from the receiving organisation in this regard, if the Authoriser deems it necessary.

[REDACTED]

4.5 Data Retention, Review and Deletion

[REDACTED]

4.5.3 A Review Panel conducts a comprehensive review of GCHQ's section 94 data, and of the directions used to acquire the data, at six-monthly intervals. The review determines whether acquisition/retention and use of each dataset remains necessary and proportionate for GCHQ to discharge its statutory functions.

4.5.4 The Panel consists of *senior GCHQ officials including a senior Legal Advisor.*

4.5.5 In conducting its review, the Panel will consider:

- the value and use of each dataset during the period under review, including specific examples that may serve to illustrate the benefits;

- the operational and legal justification for continued acquisition/retention, including its necessity and proportionality;
- 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.

4.5.6 If the Panel determines that it is no longer necessary or proportionate to retain a section 94 dataset, all copies of the data must be deleted and that must be noted in the record of the Panel. If such a determination in respect of one or more datasets means that it is no longer necessary to rely on the associated direction, that must also be noted.

4.5.7 The *relevant senior GCHQ official* will submit a six-monthly report to the Head of Intelligence Policy Department, FCO for the attention of the Foreign Secretary, together with such comments and recommendations as he sees fit. Any deletion of a dataset should be noted. If it is no longer necessary to rely on a section 94 direction, *relevant senior GCHQ official* will recommend to the Foreign Secretary that it be allowed to lapse (there being no provision in the Act to cancel a direction). The report will be copied to the Interception of Communications Commissioner.

4.5.8 The review process provides an opportunity for the Foreign Secretary to oversee the use of the directions, to seek further information or to raise concerns about any particular issues. If the Foreign Secretary agrees that a section 94 direction should be allowed to lapse, the *relevant team* will notify the relevant CNP accordingly.

4.5.9 Any deletion of a section 94 dataset will be tasked to the technical teams responsible for the relevant operational system(s). Confirmation of completed deletion must be notified to the *relevant teams*.

4.6 Oversight

Internal

4.6.1 GCHQ employees' conditions of employment make clear that "unauthorised entry to computer records" may constitute gross misconduct, subject to disciplinary measures potentially including dismissal and, in the most serious cases, referral for prosecution. Users of GCHQ IT systems are also made aware, *through the relevant policies* of their responsibilities regarding proper use of corporate IT systems.

4.6.2 All staff, contractors and integrees across the extended GCHQ enterprise are required to complete the *relevant legalities training*, which reiterates that GCHQ IT systems are to be used only for legitimate, necessary, work-related purposes and that access and use are subject to monitoring.

4.6.3 Additionally, anyone requiring access to systems containing "operational data" (which includes section 94 data) must successfully complete Advanced Legal & Policy training before accounts will be granted. This Advanced training contains detailed sections on necessity and proportionality and on N&P Statements (including audit – see below).

4.6.4 Activity on operational systems holding section 94 data is subject to audit, both from a security perspective (to ensure that no inappropriate access or misuse of access is taking

place) and to verify that legitimate access is being properly justified with respect to necessity and proportionality.

4.6.5 The latter is termed "N&P audit" and looks specifically at the reasons and justifications for running queries and searches in data held on the systems in question. Before submitting a query, the analyst is required to enter into the system a clear explanation of:

- the operational purpose in connection with which the query is made;
- how the query relates to that purpose;
- why it is necessary to run that particular query; and
- how the interference with the right to privacy the query will cause is proportionate to the outcome it is expected to achieve.

4.6.6 Queries and justifications are centrally logged and are subject to N&P audit.

4.6.7 All reports on security audit investigations are made available to the Interception of Communications Commissioner. Any incident where a member of staff has abused his/her access to communications data will be brought to the attention of the Commissioner.

4.6.8 The *relevant senior GCHQ official* will keep GCHQ's Executive Committee, of which she is a member, apprised of any pertinent issues relating to section 94 data.

External

4.6.9 The Interception of Communications Commissioner is responsible for overseeing the necessity and proportionality of section 94 directions given by the Secretary of State; the access to and use of the data acquired pursuant to the directions; the arrangements put in place for the retention, disclosure, storage and destruction of the data; and the controls and safeguards against misuse of the data. The Commissioner will normally discharge his responsibilities through his regular six-monthly inspection visits to GCHQ, or as may be otherwise agreed between the Commissioner and GCHQ.

4.6.10 The *relevant team* coordinates the Commissioner's inspection visits and makes available to him copies of the section 94 directions and associated paperwork (as required), and a copy of the latest six-monthly review. Any additional papers requested by the Commissioner must also be made available to him.

4.6.11 The Commissioner submits a report to the Prime Minister biannually, although he may choose to report on section 94 matters on an annual basis.