

Underlining indicates gisting for OPEN disclosure

Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

- (1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
- (2) SECRETARY OF STATE FOR THE HOME DEPARTMENT
- (3) GOVERNMENT COMMUNICATIONS HEADQUARTERS
- (4) SECURITY SERVICE
- (5) SECRET INTELLIGENCE SERVICE

Respondents

CLOSED RESPONSE OF THE RESPONDENTS
TO THE CLAIMANTS' REQUEST FOR FURTHER INFORMATION
AND DISCLOSURE DATED 15 JANUARY 2016

The Respondents set out below their Response to Requests 0.1 and 12 in the Claimants' Request of 15 January 2016. For the avoidance of doubt, where a Request relates to the past, the Respondents have responded in accordance with the date range directed by the Tribunal at the directions hearing on 15 January 2016, namely from 1 June 2014, except where otherwise indicated.

Of paragraph 22

"Directions have been issued under section 94 of the Telecommunications Act 1984 requiring communications service providers ("CSPs") to provide bulk communications data ("BCD"), which has subsequently been stored and accessed by the Intelligence Services ("the Section 94 regime")

0.1 Was the Section 94 regime (i.e. that section 94 TA had been used to acquire bulk communications data from UK CSPs in relation to UK customers, outside the section 8(4) regime) disclosed to the Investigatory Powers Tribunal in CLOSED in *Liberty/Privacy* [2015] 3 All ER 142, or in any other claim before the Tribunal?

The Section 94 regime and the existence of s.94 directions was not referred to in the Respondents' submissions in *Liberty/Privacy*, as those matters were not relevant to the issues in those proceedings. However, for the avoidance of doubt, GCHQ's Compliance Guide was exhibited in full to the CLOSED GCHQ witness statement which was filed in *Liberty/Privacy*. That contained passages which referred to the use of section 94 directions to obtain bulk communications data e.g. in the "Authorisations", "Collection and data acquisition" and "Communications Data" sections of the Compliance Guide, which have been disclosed again in the present proceedings.

12 For each of the Intelligence Services and each set of Handling Arrangements, please state:

- (a) The number of instances of non-compliance that have been detected;
- (b) The number of staff members identified as responsible;
- (c) The number of staff who have been (i) prosecuted; (ii) dismissed; and (iii) otherwise disciplined for non-compliance; and
- (d) The means by which the instances of non-compliance were detected.

Security Service

BPD Regime

- (a) In the period 1 June 2014 to 9 February 2016 six instances of non-compliance were detected:
 - i. Three of these were instances of datasets being mistakenly left out of the Security Service's BPD review process, with the result that the necessity and proportionality of retention was not re-considered for between one and two years;
 - ii. A further instance where a dataset which fell within the definition of "bulk personal dataset" had not been entered into the BPD process. This dataset has now been deleted;
 - iii. Two cases of individual non-compliance by staff members.
- (b) As responsibility for BPD compliance is shared between the business, information management and technical teams, it is assessed that 12 staff members hold an element of responsibility for the non-compliance referred to at (a)(i) and (a)(ii) above. In respect of (a)(iii) the responsibility was of two individuals (one on each occasion).

(c) Two of the individuals referred to at (a) have been subject to disciplinary procedures.

(d) Of the non-compliance referred to at (a) above:

a. Of the instances of non-compliance referred to at (a)(i), one was self-reported and the others were uncovered following further investigation by the Security Service's information management team;

b. The non-compliance referred to at (a)(ii) was identified following a review of BPD holdings;

c. The two instances of non-compliance referred to at (a)(iii) were identified by the Security Service's protective monitoring team.

Section 94 Regime

(a) In the period 1 June 2014 to 9 February 2016 47 instances of non-compliance either with the MI5 Closed Section 94 Handling Arrangements, or internal guidance or the Communications Data Code of Practice, were detected. These involved:

i. Four errors involving issues with the necessity and proportionality case which was made for the request for Communications Data from the database pursuant to section 22 of RIPA, e.g. insufficient consideration of data relating to an individual in a sensitive profession.

ii. 43 errors involving (i) mistransposed digits in selectors; (ii) selectors that did not relate to the subject of investigation; and (iii) occasions where duplicate requests were made.

(b) As Communications Data requests commonly have a requester and an approver, it is assessed that 94 staff members hold an element of responsibility for these instances of non-compliance.

(c) No staff members have been prosecuted, dismissed or disciplined in relation to these instances of non-compliance.

(d) These instances were self-reported by the originator of the request following detection either by the originator, the authorising officer or a third party (e.g. a team member).

Secret Intelligence Service

BPD Regime

(a) During the period 1 June 2014 to November 2015 five instances of non-compliance were detected:

- i. Two of these were instances of datasets being ingested into the system before they were authorised. In both cases, they were removed as soon as the error was detected. [REDACTED]
- ii. Three cases of individual non-compliance.

(b) In respect of (a)(i) above, the two instances occurred as a result of an ambiguity with SIS's IT systems, rather than being ascribable to any staff member's failure to comply. In respect of (a)(ii) above, three staff members were identified as responsible;

(c) None of the three staff members were prosecuted or dismissed, but the three referred to at (a)(ii) above were disciplined for non-compliance;

(d) The three instances of non-compliance referred to at (a)(ii) above were identified by SIS's Information Security audit team.

GCHQ

BPD Regime

(a) Two instances of non-compliance have been detected:

- i. The first case concerns a BPD which was acquired in 2012. The acquisition was approved, and the relevant BPDAR signed. However, the dataset was not subsequently reauthorized or considered by the BPD Review Panel, as was required. This oversight was discovered in 2015 by GCHQ's Compliance Team, who then contacted the dataset's data owners. The dataset was deleted in August 2015 as it was deemed to be no longer of use.
- ii. The second case was a BPD which was first acquired by GCHQ in 2010. However, it was not initially recognised as BPD. It was subsequently identified as BPD in 2015 by GCHQ's

Compliance Team in the context of using the data for training purposes. It was then brought within the BPD Regime and subjected to the relevant safeguards, forms and oversight.

(b) The instances of non-compliance were corporate, rather than individual. It is therefore not possible to ascribe responsibility to particular individuals. For the same reason there has been no disciplinary action.

(c) There have been no prosecutions, dismissals or disciplinary action.

(d) See (a) above.

Section 94 Regime

(a) There have been no instances of non-compliance with the GCHQ Closed Section 94 Handling Arrangements.

(b) See (a) above.

30 March 2016

**JAMES EADIE QC
ANDREW O'CONNOR QC
RICHARD O'BRIEN**

