PRIVACY INTERNATIONAL

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others

Briefing on our legal case

August 2019

Summary

The UK Security and Intelligence Agencies (SIAs) – including Government Communications Headquarters (GCHQ), Security Service and Secret Intelligence Service – have been building massive comprehensive datasets of information on each and every individual. They have been collecting and combining information from multiple sources on unclear legal bases and with minimal oversight. The majority of individuals caught in these bulk datasets are unlikely to be threats to national security. The categories of information collected are very broad.

- **Bulk personal datasets (BPDs)** contain any personal data, such as passport information, social media activities, travel data, the finance-related activity of individuals and other.
- **Bulk communications data (BCD)** describe information regarding the "who, when, where and how" of any communication including internet activity and telephone calls. They include traffic data (information attached to, or comprise in, the communication which tells something about how the communication was sent) and service data/service use information (this includes billing and other types of service use information). Subscriber information is also considered part of communications data. Examples of communication data include: all information regarding an email apart from the content of communications, map searches, visited websites, GPS location and information about every device that is connected to every Wi-Fi network.

The existence of BPDs was first publicly disclosed on 12 March 2015, when the Intelligence and Security Committee (ISC) published its report 'Privacy and Security: A modern and Accountable Legal Framework' (The ISC Report). The collection of BCD was avowed on 4 November 2015 on the publication of the draft Investigatory Powers Bill. It was also then publicly confirmed that section 94 of the Telecommunications Act 1984 (Act 1984) has been used to require telecommunications companies to provide bulk access to communications data (and potentially, bulk personal data). In addition, the Handling Arrangements for BPDs and for section 94 of Act 1984 were also disclosed, redacted in part.

Privacy International challenged the acquisition, use, retention, disclosure, storage and deletion of BPDs and BCD by UK SIAs before the Investigatory Powers Tribunal (IPT) on 8 June 2015. The claim was amended twice in the process (last one on 8 January 2016).

In its first judgment, on 17 October 2016, the IPT determined that, as a matter of domestic law, section 94 was a lawful legal basis for obtaining BCD. However, it concluded that prior to their avowal neither BPDs nor BCD was foreseeable or accessible to the public and therefore, they were not in accordance with the law as required by Article 8 of the European Convention on Human Rights. As a result, the use of BPDs was illegal prior to 12 March 2015 and the use of BCD was illegal prior to 4 November 2015. In addition, the IPT concluded that the use of BCD before the 4 November 2015 Handling Arrangements also lacked an adequate system of supervision. On the contrary, it found that the BPDs had an adequate oversight mechanism. For the post avowal period, the IPT found that both BPDs and BCD regimes were in accordance with law. A number of outstanding issues were adjourned to subsequent hearings, including the determination whether the SIAs' actions are proportionate as required by Article 8 ECHR and to consider whether BPDs and BCD are in compliance with EU law.

See also: PI Feature, PI Press Release

On 8 September 2017, the IPT decided to refer questions concerning the collection of BCD by the SIAs from mobile network operators to the European Court of Justice of the European Union (ECJ). Privacy International claimed that the regime was unlawful under EU law because it failed to provide various safeguards identified as required in the ECJ judgment in *Watson/Tele2* cases. The Government argued that the regime was outside the scope of the EU given that it related to national security (and not serious crime purposes at issue in *Watson/Tele2*) and alternatively that Article 8, ECHR provided sufficient safeguards and the implementation of *Watson* safeguards would cripple the SIAs ability to operate the BCD and should not apply. The IPT referred both topics to the ECJ.

See also: PI Feature

On 23 July 2018, the IPT issued its third judgment with respect to this case. First, the IPT concluded that there has been an unlawful delegation of statutory powers of the Foreign Secretary to the GCHQ under section 94 relating to the obtaining of BCD until 14 October 2016. This conclusion partially overturned the 17 October 2016 judgment – only with regard to BCD and only with regard to the question of whether the regime was in accordance with law. Crucial to the conclusion with respect to the legality of directions before 14 October 2016 was the revelation that a GCHQ witness had not given an accurate picture of the process under which the directions prior to 14 October 2016 have been made and implemented. This error gave the opportunity to Privacy International to cross-examine the witness during an open hearing in February 2018. Second, with regard to intelligence sharing of BPDs and BCD with foreign agencies, law enforcement agencies and industry partners, the IPT concluded that there are sufficient safeguards in place for all three Agencies. Third, the IPT decided that the acquisition and use of BPDs and BCD were proportionate as required by Article 8 of the European Convention on Human Rights.

See also: PI Press Release

On 26 September 2018, the IPT made a determination in Privacy International's favour and concluded that:

- GCHQ and SIS held BPD data related to Privacy International in the pre-avowal period – 12 March 2015. GCHQ and SIS did not access or examined that data.
- GCHQ held BCD data related to Privacy International in the period prior to 16 October 2016. GCHQ did not access or examined that data.
- Security Service held BPD data related to Privacy International in the pre-avowal period – 12 March 2015. Security Service has accessed or examined such data.
- Security Service held BCD data related to Privacy International in the pre-avowal period – 4 November 2015. Security Service has accessed or examined such data.

The Security Service announced that they destroyed the data relating to Privacy International that it held in the 'Workings' area of its system the day before the hearing on 25 September 2018. As a result, it will not be possible to

See also: PI Press Release

Timeline of case

12 March 2015
The Intelligence and Security Committee published its report 'Privacy and Security: A modern and Accountable Legal Framework' that disclosed for the first time the existence of bulk personal datasets (BPDs).

8 June 2015
Privacy International submitted a case challenging the acquisition and use of BPDs by Security and Intelligence Agencies (SIAs) – particularly the Government Communications Headquarters (GCHQ), Security Service (MI5) and Secret Intelligence Service (SIS). The claim contested the legality of BPDs under the European Convention on Human Rights.

10 September 2015
The claim was amended to include the use of section 94 of the Telecommunications Act 1984 (1984 Act) to require communications and service providers to provide bulk access to communication data without a clear framework and no meaningful or effective oversight regime. It was at this stage that the bulk communication data (BCD) component was introduced in the case, as well as challenging the compliance of these practices with EU law (next to human rights law).

4 November 2015
The publication of the draft Investigatory Powers Bill confirmed the use of section 94 of the Telecommunications Act 1984 to require telecommunications companies to provide bulk access to communication data. In addition, the Handling Arrangements regulating the acquisition and use of BPDs and BCD were published.

8 January 2016
The claim brought by Privacy International was re-amended to include the above developments.

17 October 2016
First Investigatory Powers Tribunal (IPT) judgment concluding that both BPDs and BCD lacked sufficient foreseeability or accessibility until their public disclosure – on 12 March 2015 and on 4 November 2015 respectively – and therefore were not in accordance with law. As such they breached Article 8(2) of the European Convention on Human Rights. A number of outstanding issues were adjourned to a subsequent hearing, including whether the Agencies' actions were proportionate, in accordance with Article 8(2) ECHR and whether they were in accordance with EU law.

12 December 2016
IPT ordered the SIAs to carry out searches for identifiers related to Privacy International in their BPDs and BCD and to provide a report detailing the results of those searches.

17 February 2017
First SIAs report on searches confirming that both the Security Service and Secret Intelligence Service search results showed that they held data relating to Privacy International in their BPDs prior to their avowal on 12 March 2015. None of the SIAs held any relevant BCD data. These statements were corrected multiple times later on.

8 September 2017
Second IPT judgment referring to the Court of Justice of the EU (CJEU) questions concerning the compliance of the BCD collected by providers of electronic communications networks with European Law standards.

6 October 2017
First amendment of SIAs report on searches recognising that the Security Service did, in fact, hold data relevant to Privacy International in its BCD prior to their avowal on 4 November 2015.

26 February 2018
First ever cross-examination of a GCHQ witness by Privacy International on serious misleading errors provided to the Tribunal in previous statements in relation to BCD.

23 July 2018
Third IPT Judgment concluding that for a sustained period successive Foreign Secretaries wrongly gave GCHQ unfettered discretion to collect vast quantities of BCD from telecommunications companies. As a result, it partially amended its judgment of 17 October 2017 to conclude that BCD operated in violation of Article 8(2) ECHR until 14 October 2016. IPT found that both BPD and BCD complied with the requirement of proportionality of Article 8(2) ECHR. Finally, the Tribunal concluded that the sharing of BPD and BCD with foreign agencies, law enforcement agencies and industry partners complied with Article 8 ECHR.

17 February 2018
SIAs re-amended the report on searches with respect to Privacy International's data confirming that all three agencies held (or, in the case of GCHQ, more likely than not held) data relating to Privacy International in their BPDs, prior the 12 March 2015 disclosure. In addition, both GCHQ and the Security Service reported that they held data relating to Privacy International in their BCD while the regime was unlawful (that is before 16 October 2016). It was additionally revealed, in a separate response, that the Security Service had selected data relating to Privacy International for analysis as part of an investigation and stored it in an area referred to as 'Workings' which stores the results from searches which officers have been undertaking, as part of their investigation. Data in 'Workings' seems to be indefinitely stored, with no determined period for review or deletion.

24 September 2018
Security Service deletes data relating to Privacy International that it held in the 'Workings' area of its system.

26 September 2018
On 26 September 2018, IPT made a determination in Privacy International's favour and concluded that GCHQ, Security Service and SIS held data related to Privacy International in the pre-avowal period – 12 March 2015. Security Service had in addition accessed or examined such data. Also, GCHQ and Security Service held BCD data related to Privacy International in the period prior to 16 October 2016. Security Service had accessed or examined such data. Also, confirmed that Security Service destroyed BPD and BCD data relating to Privacy International that it held in the 'Workings' area of its system.

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471