



BRIEFING ON LEGAL CASE
Privacy International v
Secretary of State for Foreign and
Commonwealth Affairs and others

July 2021

[privacyinternational.org](https://www.privacyinternational.org)

Summary

The UK Security and Intelligence Agencies (SIAs) – including the Government Communications Headquarters (GCHQ), the Security Service (MI5) and the Secret Intelligence Service (MI6) – 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 whose personal data is caught by these bulk datasets are unlikely to be threats to national security. The categories of information collected are very broad.

- **Bulk personal datasets** contain any personal data, such as passport information, social media activities, travel data, the finance-related activity of individuals.
- **Bulk communications data** describes information relating to the “who, when, where and how” of any communication, but not the content of the communication itself. The types of communication include internet activity and telephone calls. Communications data therefore includes traffic data (which is information attached to, or comprised in, the communication which reveals 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 the email itself), digital map searches, visited websites, GPS location and information about any device that is connected to any Wi-Fi network. In the UK, the legal definition of “communications data” is contained in s.261(5) of the Investigatory Powers Act 2016.

Notably, prior to 2015, there had never been any public disclosure by the UK’s security and intelligence agencies that they collect and hold bulk personal datasets (BPD) and bulk communications data (BCD). The existence of BPDs was first publicly disclosed on 12 March 2015, when the parliamentary Intelligence and Security Committee (ISC) published its report [‘Privacy and Security: A modern and Accountable Legal Framework’](#) (the ISC Report). Additionally, the collection and existence of BCD was revealed publicly 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 (the 1984 Act) has been used to require telecommunications companies to provide the SIAs with bulk access to communications data (and potentially, bulk personal data). In addition, the policies containing safeguards around how SIAs must handle both BPDs and BCD obtained under section 94 of the 1984 Act, which are known as the “Handling Arrangements” were also disclosed for the first time in November 2015, although redacted in part.

Privacy International first filed its challenge related to 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, and the final amendment to the claim was filed on [8 January 2016](#).

The IPT’s judgement was given in three parts, and a final declaration on points of EU law was made by the IPT in July 2021.

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 also concluded that

before it became public knowledge that SIAs collected and retained BPDs and BCDs (in the judgement, this is referred to as prior to “avowal”), neither BPDs nor BCD were foreseeable or accessible to the public and therefore, the regimes governing the acquisition, use, retention, disclosure, storage and deletion of BPDs and BCD by UK SIAs during that time period were not in “accordance with the law” as required by Article 8 of the European Convention on Human Rights. As a result, the SIA’s use of BPDs was illegal prior to 12 March 2015, and the SIA’s use of BCD was illegal prior to 4 November 2015. In addition, the IPT concluded that the use of BCD before the publication on 4 November 2015 of the relevant “Handling Arrangements” also lacked an adequate system of supervision. However, and specifically in relation to BPDs, the IPT found that the regime included an adequate oversight mechanism during the pre-avowal period. In assessing the lawfulness of the regimes following the public disclosures around SIA’s retention and use of BPDs and BCD, the IPT found that both the BPDs and BCD regimes were in accordance with law. A number of outstanding issues were adjourned to subsequent hearings, including the determination around whether the SIAs’ actions were proportionate as required by Article 8 ECHR and the assessment as to whether BPDs and BCD regimes were in compliance with EU law.

See also: [PI Feature, 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 Court of Justice of the European Union (CJEU). Privacy International argued that the regime was unlawful under EU law because it failed to provide various safeguards which had been held to be a requirement under EU law according to the CJEU’s judgment in the [Watson/Tele2 cases](#). The Government argued that the BCD regime was outside the scope of EU law given that it related to national security (and not serious crime purposes as was at issue in *Watson/Tele2*). The UK government also argued that Article 8 of the ECHR provided sufficient safeguards, and that the implementation of the *Watson* safeguards would cripple the SIAs ability to operate the BCD and therefore, should not apply. The IPT referred both issues to the CJEU.

See also: [PI Feature](#)

On [23 July 2018](#), the IPT issued its third judgment with in this case. First, the IPT concluded that there had been an unlawful delegation of statutory powers by 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 SIAs sharing BPDs and BCD with foreign agencies, UK law enforcement agencies and industry partners (including researchers or contractors), 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 favour of Privacy International and concluded that:

- GCHQ and SIS (MI6) held BPD data related to Privacy International in the pre-avowal period – 12 March 2015. GCHQ and SIS (MI6) did not access or examine that data.
- GCHQ held BCD data related to Privacy International in the period prior to 16 October 2016. GCHQ did not access or examine that data.
- MI5 held BPD data related to Privacy International in the pre-avowal period – 12 March 2015. MI5 has accessed or examined such data.
- MI5 held BCD data related to Privacy International in the pre-avowal period – 4 November 2015. Security Service has accessed or examined such data.

MI5 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.

See also: [PI Press Release](#)

On [6 October 2020](#), the Court of Justice of the European Union (CJEU) issued its judgment in the case following the request for a preliminary ruling by the IPT on [8 September 2017](#) (C-623/17). In that referral, the IPT asked the CJEU whether (i) the bulk communications regime was within the scope of EU law and, if so, (ii) whether additional safeguards applied beyond those established by the European Convention of Human Rights. The CJEU answered both questions in the affirmative. It ruled that mass data retention and collection practices for national security purposes undertaken by member states, must comply with EU law, and therefore must be subjected to its privacy safeguards.

See also: [PI Press Release](#), [PI Q&A](#)

On [22 July 2021](#), the IPT issued a declaration finding that scheme for the collection of BCD under section 94 of the Telecommunications Act 1984 (which has since repealed by the Investigatory Powers Act 2016) was incompatible with EU law human rights standards. The result of the judgment is that a decade’s worth of secret data capture has been held to be unlawful. The unlawfulness would have remained a secret but for PI’s work.

See also: [PI News&Analysis](#)

In January 2020 Privacy International and UK-based NGO Liberty [filed a new claim](#) against MI5 and the Secretary of State for the Home Department in the Investigatory Powers Tribunal (the “Ungoverned Spaces Case”, this time, the case sought to hold MI5 and the SSHD accountable for systemic, long-term failures in the way they handle and retain millions of people’s personal data. As part of this claim, PI requested that the IPT re-opens parts of the original BPD/BCD. This aspect of the Ungoverned Spaces Case is still ongoing.

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

The 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.

31 January 2020

Privacy International and UK-based NGO Liberty [file a new claim](#) against MI5 and the Secretary of State for the Home Department in the Investigatory Powers Tribunal (the “Ungoverned Spaces Case”, this time, the case sought to hold MI5 and the SSHD accountable for systemic, long-term failures in the way they handle and retain millions of people’s personal data. As part of this claim, PI requested that the IPT re-opens parts of the original BPD/BCD. This aspect of the Ungoverned Spaces Case is still ongoing.

6 October 2020

Court of Justice of the European Union’s (CJEU) judgment on the case following the request for a preliminary ruling by the IPT on 8 September 2017 (C-623/17) where it ruled that mass data retention and collection practices for national security purposes undertaken by member states, must comply with EU law, and therefore must be subjected to its privacy safeguards.

22 July 2021

The IPT issued a declaration finding that section 94 of the Telecommunications Act 1984 (since repealed by the Investigatory Powers Act 2016) was incompatible with EU law human rights standards.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org