PRIVACY INTERNATIONAL

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

Summary of legal proceedings

August 2019

BPD-BCD Legal challenge: Summary of legal proceedings

In these proceedings, Privacy International challenged the acquisition, use, retention, disclosure, storage and deletion of bulk personal datasets (BPDs) and bulk communications data (BCD) by the UK Security and Intelligence Agencies (SIAs). The existence of BPDs and BCD were initially secret (on the disclosures see below).[1] BPDs and BCD are comprehensive datasets of information on each and every individual. They contain data about individuals, the majority of whom are unlikely to be threats to national security.

What information do these datasets include?

- BPDs are datasets that contain personal data about individuals. Personal data describe any personal information about an individual, such as passport information, social media activities, travel data, the finance-related activity of individuals and other.
- BCD are data that contain information regarding the "who, when, where and how" of any communication, including internet activity and telephone calls. It describes all information around a communication apart from the content of the communications. For example, it includes the visited websites, email contacts, to whom, where and when an email is sent, map searches, GPS location and information about every device connected to every Wi-Fi network.
    - The Intelligence agencies claimed they collect traffic data (information attached to, or comprised in, the communication which tells you something about how the information is sent) and service data/service use information (this includes billing and other types of service use information [ISC Report 2015]). The reference to the CJEU refers only to 'Traffic Data' and 'Service Use Information'. The Intelligence Agencies claim that the absence of communication content or subscriber information means that the communications data 'cannot be ascribed to an individual, taken alone'.[2]
    - However, we know that GCHQ was also acquiring subscriber information (information held or obtained by a communications service provider about persons to whom a communications and service provider offers a service) under section 94 of the Telecommunications Act 1984 until 2015[3]. Also, the Security Service was using RIPA to obtain subscriber information (2013 ISC Report).
      On communications data see PI website here and here.

[1] The agencies claimed that such datasets are crucial for monitoring known and high-priority threats but also to discover new targets and identify emerging powers. However, there are no concrete evidence to support such claim.

[2] Respondents Skeleton Argument, 30 May 2017, para 25.1.

[3] As set out in the Report of the Interception of Communications Commissioner, Review of directions given under section 94 of the Telecommunications Act 1984, Sir Stanley Burnton stated in para 8.35: "IOCCO Identified that a PECN had historically been required (since 2001) to supply subscriber information to GCHQ in addition to traffic data as part of a section 94 direction. The subscriber information obtained pursuant to this section 94 direction was destroyed in October 2015. The Operational Case for Bulk Powers published in March 2016 by the Government does not set out an operational requirement or case for bulk subscriber information. The agency handling arrangements for the acquisition of bulk communications data published in November 2015 state clearly that: "The communications data collected is limited to "Traffic Data" and "Service Use Information". "The data provided does not contain communication content or Subscriber Information.""

On which legal basis is this information collected?

- The authority of agencies to acquire and retain BPD is not clearly defined in legislation. BPDs are acquired from various sources justified on different legal bases. It can be personal information obtained by warrant, by section 20 of RIPA, by section 5 and section 7 of the Intelligence Services Act 1994, and possibly section 94 of the Telecommunications Act 1984.
- BCD have been acquired by GCHQ and Security Service through a number of section 94 directions (GCHQ since 1998-1999 and MI5 since 2005).[4]
  On section 94 Act 1984, see PI legal analysis.

By whom is data collected?

Information fed into a BPD most probably may come from various sources, but it is not clear from the case. Information in BCD is acquired through communications and service providers (CSPs) under section 94 of Act 1984. A CSP can be a company such as BT, Vodafone or Virgin Media, that provides access to internet and telephony services through its network infrastructure (Intelligence & Security Report 2013).

Avowals and evolution of Privacy International's claim

On 12 March 2015, the Intelligence and Security Committee (ISC) published its report 'Privacy and Security: A modern and Accountable Legal Framework' (The ISC Report). The ISC Report disclosed for the first time the existence of the BPDs (see paras 151-163, ISC Report). The report underlined that these BPDs concern large numbers of people and have been established and operating with minimal oversight and no clear regime governing them (p 59, ISC Report). One day before, on 11 March 2015, the Prime Minister signed the Intelligence Services Direction 2015 that acknowledged that BPDs comprise personal data that relate to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest. [Statement repeated in the 11 April 2016 response by the respondents in the course of the legal proceedings.]

On 8 June 2015, Privacy International brought the case against the Secretary of State for Foreign and Commonwealth Affairs (Foreign Secretary), the Secretary of State for the Home Department (Home Secretary) and the three Security and Intelligence Agencies (Government Communications Headquarters (GCHQ), the Security Service (MI5), and the Secret Intelligence Service (MI6)) with regard to BPDs before the Investigatory Powers Tribunal (IPT).

The claim was amended twice over the course of the judicial proceedings before the IPT. First, on 10 September 2015, the claim was amended to include section 94 of the Telecommunications Act 1984 (1984 Act) that permits the Home Secretary to give national security directions to Ofcom and providers of public electronic communications networks (PECNs). The amendment was made before the public avowal of the use of section 94 (para

[4] Copied from Privacy International website: 'These directions are general, surrounded by secrecy, not time bound and not reviewed independently. They have been used by the intelligence agencies to collect Communications Data outside Regulation of Investigatory Powers Act 2000 (RIPA) powers, unhindered by the Home Office's Statutory Code of Practice on Communications Data Acquisition.'

12, re-amended claim).[5] It was at this stage that the BCD component was introduced in the case, as well as challenging the compliance of these practices with EU law (next to human rights law). The claim was further amended after the avowal.

On 4 November 2015, section 94 directions and BCD were disclosed on the publication of the draft Investigatory Powers Bill. It was then publicly confirmed that section 94 has been used to require telecommunications companies to provide bulk access to communications data (and potentially, bulk personal data). In addition, "Handling Arrangements for BPD and for s.94 were both published on 4 November 2015, and were supplemented by Closed Handling Arrangements in relation to each of the SIAs, which have been subsequently, during the course of these proceedings, disclosed, redacted in part." (para 15, IPT October 2016, see below). As a result of the avowal, the claim was re-amended on 8 January 2016, to include these developments (para 13, re-amended claim).

Judgments

17 October 2016

The IPT published 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 (para 58, IPT October 2016). With respect to the compliance of these datasets with human rights principles, the decision is split between the use of these datasets prior to and post their respective avowal.
For prior to its avowal period (before 12 March 2015[6]), the IPT concluded that BPDs failed to comply with the principles of the European Convention on Human Rights (ECHR). Similarly, the IPT decided that BCD also failed to comply with the ECHR principles in the period prior to its avowal on 4 November 2015.
Specifically, the IPT concluded that both BPDs and BCD were not foreseeable by or accessible to the public, since they were never explained to the public, none of the rules or arrangements disclosed by the respondents were previously disclosed or signposted, prior to the publication of the Handling Arrangements in November 2015 (para 71, IPT October 2016).[7] Therefore, they were not 'in accordance with law' as required by Article 8(2) ECHR. In addition, the IPT concluded that BCD also lacked an adequate system of supervision before the 4 November 2015 Handling arrangements (paras 80 & 84, IPT October 2016). On the contrary, it found that BPDs had an adequate oversight mechanism (paras 82 & 84, IPT October 2016) (see in detail paras 67-84 & 101, IPT October 2016). For the post avowal period, the IPT found that both BPDs and BCD were in accordance with law (paras 94 & 100, IPT October 2016).
A number of outstanding issues were adjourned to subsequent hearings, including to determine whether the SIAs' actions were proportionate as required by Article 8 ECHR and to consider whether BPDs and BCD are in compliance with EU law.

[5] The amended claim referred to the book of Gordon Corera, *Intercept: The Secret History of Computers and Spies* (2015), p 332 as a source of the use of section 94 for BCD.
[6] NB the IPT refers to the date of publication of a Direction by the PM as the avowal date which was 11 March 2015, but it refers to 12 March in its final paras of the judgment, see para 13, IPT, October 2016
[7] While the Handling arrangements were published for both BPD and BCD on 4 November 2015 and the IPT uses this argument to conclude on the two regimes 'foreseeability', the IPT eventually concludes that the BPD was in accordance with law as of 12 March 2015 and not 4 November 2015 (para 71 read in conjunction with paras 84 & 100, IPT October 2016).

Para 5, IPT October 2016:

- BCD is acquired by GCHQ and MI5 under s 94
- BPDs is acquired and used by GCHQ, MI5, MI6 through various sources (including potentially s 94)
- BCD+BPDs can be searched by all SIAS to discover about persons of intelligence interest.

See also: PI Feature, PI Press Release

8 September 2017

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 claimed that BCD were unlawful under EU law because it failed to provide various safeguards identified as required in the CJEU judgment in *Watson/Tele2* cases. The Government argued that BCD were 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 of the ECHR provided sufficient safeguards and the implementation of *Watson* safeguards would cripple the SIAs ability to operate BCD and so should not apply. The IPT referred to both topics to the CJEU. Its preliminary conclusions though were that actually issues of national security fell outside the scope of EU law (para 35, CJEU referral) that the CJEU might have erred in its approach in *Watson* case and also that it was not clear how *Watson* safeguards could or would apply in this context (para 56, CJEU referral).

See also: PI Feature and PI Website on CJEU proceedings

23 July 2018

On 23 July 2018, the IPT issued its third judgment with respect to this case. It addressed several issues. 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 whether they were in accordance with law (para 58, IPT July 2018).[8] According to the IPT, on 14 October 2016 new directions replaced the former directions made under section 94. The new directions were more specific as to the categories of communications data required by the Director of GCHQ (para 37, IPT July 2018).[9] Crucial to the conclusion with respect to the legality of

[8] The IPT however decided that it was not necessary to propose to quash any directions or to make any declaration as to their effect. Among others, the IPT considered the fact that from 2014 onwards in substance and effect there was no unlawful delegation of power, nor was there a disproportionate use of such directions; fearing potential effects on third parties, the CSPs and it would not be in position to quash some and not others (para 59, IPT July 2018).

[9] Although the IPT concluded that the general directions were not in accordance with law until 14 October 2016, it also added that in practice by 2014, it was the Foreign Secretary that 'determined the scope of data collection permitted under all directions which remained in force' (para 55, IPT July 2017). It added also that despite the broad scope of directions until October 2016 (the GCHQ had substantive powers to determine the content and the duration of the requests to the CSPs), in practice there was no evidence to support that the GCHQ sought data that were not subject of a submission to and approval by the Foreign Secretary after about 2010) (paras 51ff, IPT July 2018). In para 54, the IPT concluded that: 'The broad scope of the general directions did not in

directions before the 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. The IPT more than once in its judgment underlined the fact that on a number of occasions the GCHQ statements had to be subsequently corrected (see paras 6(iv), 12-17 & 40, IPT July 2018, see further below under hearings). With regard to the question of necessity and proportionality, though the IPT concluded that 'the acquisition of bulk communications data under lawful directions made under s.94 by the Foreign Secretary on 14 October 2016 was and remains necessary and proportionate' (para 57, IPT July 2018).

Second, in its judgment on 23 July, the IPT addressed the question of intelligence sharing regarding both BPDs and BCD (paras 61 ff, IPT, July 2018). (a) Sharing of BCD and BPD with Foreign Agencies: The IPT concluded that there are sufficient safeguards in the system in place with all three Agencies. 'No data could be shared without full prior consideration of the nature, remit and security arrangements of the proposed recipient, and without prior authorisation of a senior officer' (para 66, IPT July 2018). It further concluded that the oversight system was adequate and compliant with the requirements of Article 8 of the European Convention on Human Rights (para 71, IPT July 2018). (b) Sharing of BCD and BPD with Law Enforcement Agencies: The IPT also concluded that there were adequate safeguards and oversight in place with regard to sharing of information with Law Enforcement Agencies as well (paras 73-77, IPT July 2018). (c) Sharing with industry partners: Again, the IPT did not consider that there was a violation of Article 8 of the ECHR with respect to sharing of information with industry contractors.

However, the IPT were critical of the Intelligence Agencies in respect of the inaccurate information given to the Tribunal as to the number of such contracted with Privileged User accounts, "a failure the significance of which Dr Gus Hosein, an Executive Director of the Claimant, highlighted in pointing out the importance of the role that a Privileged User with administrative rights could play."[10]

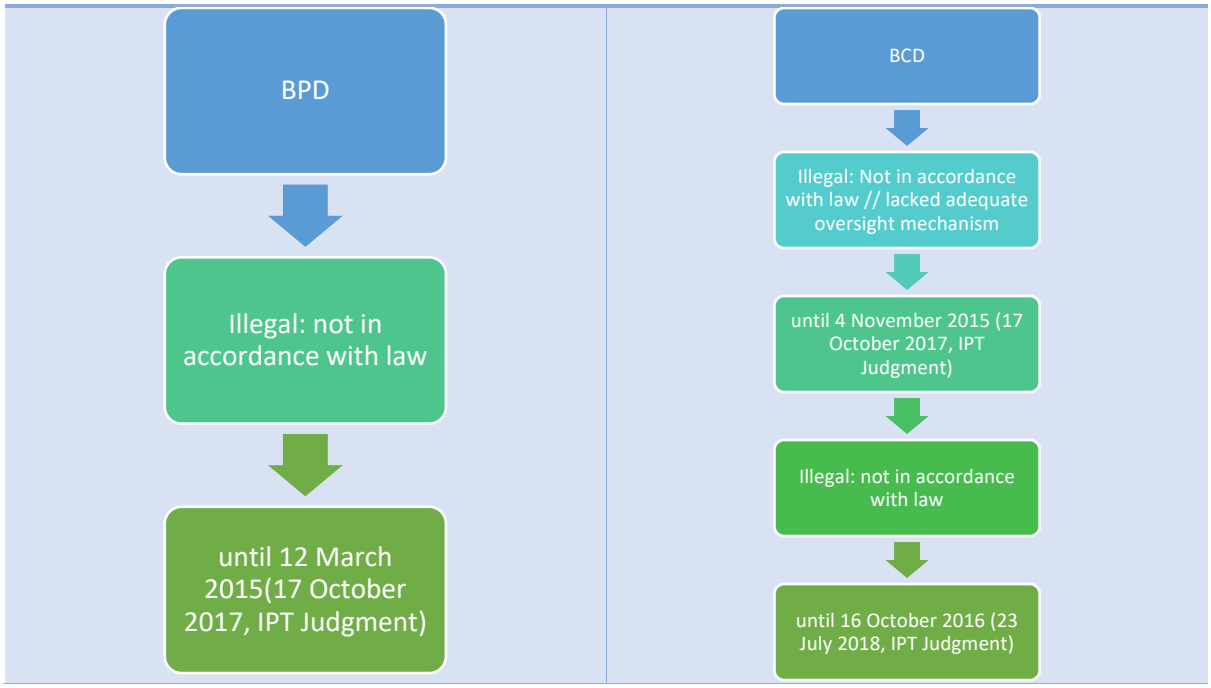
Third, the IPT decided that the acquisition and use of BPD and BCD were proportionate to the legitimate aim in accordance with Article 8 ECHR. Particularly, it concluded that 'consideration of proportionality is inbuilt into the Agencies' systems, and that there is regular consideration, at both the stage of acquisition and of access, of whether there are any practical alternative measures that could be taken' (para 93, IPT July 2018). The IPT underlined that GCHQ has been fully mindful of its obligations as to bearing in mind both necessity and proportionality in obtaining data pursuant to section 94 directions and that from what it had seen and heard in closed evidence it decided that the Respondents did indeed consider whether less intrusive means of obtaining information which can be derived from the datasets could be used (paras 91 & 93, IPT July 2018).[11]
See also: PI Press Release

practice lead to the provision of any BCD which could not lawfully have been required under s.94, within the limits prescribed by Article 8.'

[10] 23 July 2018 Judgment, para 81.

[11] The IPT considered that the issue of proportionality is entirely different from, and supplementary to, the issue of necessity. It underlined that it has no doubt that BPD and BCD is of great value in the protection of national security. The question for IPT was whether the legitimate aim of protecting national security could be equally achieved by less intrusive measures. (para 87, IPT July 2018).

IPT'S CONCLUSIONS



Orders relating to Privacy International's data

The judgments summarised above concerned the legality of the BPDs and BCD in general. In parallel to this process, the IPT issued orders to the SIAs to carry out searches in their BPDs and BCD to determining whether any Privacy International's data were caught up in these datasets. As the proceedings unfolded, the SIAs were compelled to reveal additional information with regard to the manner in which BPDs and BCD have been collected for more than a decade.

The IPT first ordered the SIAS to carry out searches for identifiers related to Privacy International in their BPDs and BCD on 12 December 2016[12] and to provide a report detailing the results of those searches. On 17 February 2017, the SIAs responded and confirmed that both the Security Service and the SIS search results showed that they held data relating to Privacy International prior to their avowal on 12 March 2015. It further stated that none of the SIAs held any relevant BCD data. On 6 October 2017, the SIAs amended their report to show that the Security Service did indeed hold data in its BCD prior to their avowal on 4 November 2015. On 17 August 2018, the SIAs re-amended their report to confirm that all three agencies held (or, in the case of GCHQ, more likely than not held) data relating to Privacy International in its BPDs, prior the 12 March 2015 avowal. In addition, both GCHQ and the Security Service reported that they held data relating to Privacy International in their BCD while they were unlawful (that is before 16 October 2016). In the Respondent's Re-Amended OPEN Response to the Claimant's request for Further Information which was served on 6 October 2017 it was additionally revealed 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

[12] Probably has been removed from the website but copy saved, Internal.

to as 'Workings' which stores the results from searches which officers have been undertaking, as part of their investigation. Data in 'Workings' is indefinitely stored, with no period for its review and deletion.

The repeated corrections of their reports demonstrated the inability of the agencies to control the information caught up in the BPDs and BCD.

Determination regarding Privacy International's data

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

- GCHQ and SIS held BPDs data related to Privacy International in the pre-avowal period – 12 March 2015. GCHQ and SIS did not access or examined that data (para 5(a) and (e), IPT Determination).
- GCHQ held BCD data related to Privacy International in the period prior to 16 October 2016. GCHQ did not access or examined that data (para 5(b), IPT Determination).
- Security Service held BPDs data related to Privacy International in the pre-avowal period – 12 March 2015. MI5 has accessed or examined such data (para 5(c), IPT Determination).
- 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 (para 5(d), IPT Determination).

!! Security Service destroyed the BPDs and BCD data relating to Privacy International that it held in the 'Workings' area of its system (para 6, IPT Determination) without any further explanation.

The determination was based on information provided in the Report on Searches and the Respondent's Re-Amended OPEN Response to the Claimant's request for Further Information which was served on 6 October 2017.

Seminal Hearing – GCHQ's Misleading Evidence

This hearing concerned the acquisition of BCD from CSPs by GCHQ under section 94. On the delegation argument, the Respondents' initially asserted that it was the Foreign Secretary, not GCHQ, who made the decision as to which communications data was required to be provided by each CSP. Specifically, based on the fourth open witness statement of the GCHQ witness (16 June 2017), the evidence showed that the GCHQ officials had no discretion as to the categories of data that were to be provided. The witness stated that '(a) the datasets to be provided were "*routinely*" set out in the submission to the Foreign Secretary, (b) requests for communications data "*were always made immediately following the making of the direction by the Foreign Secretary*", (c) in the event that GCHQ wished to change the datasets the approval of the Foreign Secretary had to be sought, and (d) no selection or alteration of datasets to be provided "*has ever been made unilaterally by the Director of GCHQ or any other official*"' (quote from para 12, IPT July 2018). That evidence formed the basis of the Respondents' submissions at paragraphs 62-68 of the skeleton argument served on 6 October 2017, which were advanced orally during the hearing on 17-18 October 2017.

On 15 December 2017, the GCHQ witness made substantial corrections to the evidence which had been set out in his fourth witness statement (Tenth witness statement of the GCHQ witness). He admitted that in a number of cases the submissions to the Foreign Secretary did not specify the data to be sought from the CSP, the directions were of a general nature and the specific data to be provided were specified by GCHQ in a trigger letter or orally. The justification for these errors was that the witness had relied on his own knowledge and it was only when the IPT requested further information that the searches revealed the relevant documentation (para 14, IPT July 2018).

Following these revelations, Privacy International asked to cross-examine the GCHQ witness and the cross-examination took place on 26 February 2018 (para 15, IPT July 2018). "The explanation of the witness for the errors in his 4th witness statement was that he had not fully read the file of relevant documents but had relied on information from others in GCHQ. That explanation was not entirely consistent with that advanced at paragraph 22 of his 10th witness statement and was surprising, given that the file of all relevant documents had apparently been compiled and made available to the IOCC for the purpose of his review which commenced in October 2015" (para 15, IPT July 2018).

As a result, in conjunction with other evidence received by the IPT in Closed, the GCHQ's initial submission could not be withheld and the IPT concluded in its judgment on 23 July 2018 that the Foreign Secretary was unlawfully delegating power to GCHQ until 16 October 2016. As a result, the BCD were unlawful until 16 October 2016.

This part of the process reveals that the government misrepresented BCD's operation with regard to its oversight mechanism and it was revealed that it did not actually have a high-level oversight mechanism.

Information from: IPT July Judgment, PI Press Notice

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