

Privacy International

Comments Submitted to the Independent Review of the Investigatory Powers Act 2016

13 March 2023

1. Introduction

- 1.1. Privacy International (PI) researches and advocates globally against government and corporate abuses of data and technology. It exposes harms and abuses, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have security and freedom through greater personal privacy.
- 1.2. PI welcomes the opportunity to provide comments to Lord David Anderson KBE KC (the “Reviewer”), as part of the independent review of the Investigatory Powers Act 2016 (the “IPA”) (the “Review”).
- 1.3. PI regularly undertakes in-depth research and analysis of emerging technologies, both over the course of the technology’s development and following its acquisition and deployment by a variety of actors, including corporate actors, malicious actors, and state actors. PI works closely with international partner organisations to produce research and evidence which explains and uncovers (a) how certain technologies work, and (b) how those technologies can and have been used to exploit and surveil certain populations, as well as restrict people’s ability to exercise their fundamental rights.¹ Over the past five years, PI has been involved in several legal challenges in the UK related to the lawfulness of mass surveillance, the acquisition and use of bulk personal data sets and bulk communication data, and the human rights implications of digital surveillance.

¹ See for example, Privacy International, [“Electronic monitoring using GPS tags: a tech primer”](#), February 2022; Privacy International, [“Telco data and Covid-19: A primer”](#), April 2020; Privacy International, [“GPS tracking and COVID-19: A tech primer”](#), May 2020; Privacy International, [“Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya”](#), March 2017; [Privacy International’s Complaint to the ICO regarding Mobile Phone Extraction technology](#), April 2018; Privacy International, [“Push this Button for Evidence: Digital Forensics”](#), June 2019; Privacy International, [“Challenge against Clearview AI in Europe”](#), May 2021; Privacy International, [“Restraining Protest Surveillance: When should surveillance of protesters become unlawful?”](#) November 2022; Privacy International, [“Micro-targeting in political campaigns: a comparative analysis of legal frameworks”](#), January 2021; Privacy International, [“The UK’s Privatised Migration Surveillance Regime: A Rough Guide for Civil Society”](#), January 2021.

1.4. The Terms of Reference of the Independent IP Review² ("ToR") set out the topics that the review will focus on, with priority to be given to the effectiveness of the Bulk Personal Dataset (BPD) regime. PI's response will focus on topics a) the effectiveness of the BPD regime and whether Part 7 remains fit for purpose; and e) the oversight regime, and ways to increase resilience and agility in light of the experience of the last five years of operation. We have further included two additional sections on omissions and general comments on the review process.

1.5. PI's comments are structured in line with the (1) the ToR; (2) the particular areas of interest referred to in the body of the text provided on the Reviewer's website;³ and (3) the list of Specific Topics provided by the Reviewer on 17 February 2023.⁴

2. Effectiveness of the Bulk Personal Datasets (BPD) regime: is part 7 fit for purpose?

2.1. Regulating the acquisition and/or use of BPDs in light of current and future technological changes and evolving threats

2.1.1. In addition to addressing the acquisition and use of BPDs in light of current and future technological change, our submissions in this section relate to chapter 3 of the Home Office Report on the Operation of the Investigatory Powers Act 2016⁵ (the "Statutory Report"), titled "Changing Operational Environment". Of course, there have been, and there will continue to be, significant technological advancements constantly reshaping the types of data and intelligence that can be generated by networked technologies and computers (that is, technologies used every day by billions of people, including mobile phones, laptops, 'smart devices', search engines and data storage systems). The same is true of the technological means available for processing these datasets – such as the growth and development of cloud computing

² Independent Review of the Investigatory Powers Act 2016, Terms of Reference, 2023, available online: <https://www.gov.uk/government/publications/independent-review-of-the-investigatory-powers-act-2016>

³ David Anderson KC KBE, "Investigatory Powers Act Review", (2023), <https://www.daac.co.uk/2023/02/09/investigatory-powers-act-review/>

⁴ David Anderson KC KBE, "IPA Review Specific Topics", 17 February 2023, available online: <https://www.daac.co.uk/wp-content/uploads/sites/22/2023/02/Specific-Topics.pdf>

⁵ Home Office, "Report on the Operation of the Investigatory Powers Act 2016", February 2023, available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1134783/E0282558_1_Investigatory_Powers_Act_2016_ELAY.pdf

and artificial intelligence (both referenced within the Statutory Report). However, none of the specific technological developments identified within the Statutory Report have led to a radical change in the UKSIC's operational environment such that it has rendered part 7 of the IPA operationally ineffective.

2.1.2. PI does not consider that, in the period between 2016 and 2023, there has been an emergence of technological change or an evolution of technology such that the objectives of the IPA, and in particular the objectives of part 7, can no longer be met as currently drafted.

2.1.3. The "digitisation reshaping our societies and economies" which is referred to at page 14 of the Statutory Report has been apace since, at least, the commercialisation of wireless mobile network technologies and the Internet from the late 1990s onwards. Importantly, the Reviewer's own report titled "A Question of Trust" which was undertaken specifically to inform the legislative debate around the Investigatory Powers Bill, addressed, at length, trends related to digital technology, 'big data', the 'Internet of Things' and machine learning.⁶ If the term 'digitisation' in the Statutory Report is intended to refer to the globalised shift from analogue transmission in telecommunications, and more generally, analogue modes of creating and recording personal data points, to digital transmission of telecommunications and, subsequently, digital production of (infinite) data points which record human activity, there is no evidence to support the proposition that the particular technological shifts which have taken place between 2016 and 2023 were not well understood, widely researched and in fact, already taking place prior to 2016.⁷

2.1.4. Specifically in relation to the BPD regime, the Statutory Report argues that there has been an "exceptional growth in volume and types of data across all sectors of society globally since the Act entered into force"⁸ and that "the

⁶ David Anderson KC (Independent Reviewer of Terrorism Legislation), *"A Question of Trust: Report of the Investigatory Powers Review"*, June 2015, pp. 49-70.

⁷ See for example, Stephen Saxby, "The Age of Information: the Past Development and Future Significance of Computing and Communications" (1990) Palgrave Macmillan; David H. Flaherty, "Protecting Privacy in Surveillance Societies" (1989) UNC Press; Electronic Privacy Information Center and Privacy International, *"Threats to Privacy"* pp. 21 – 189, in "Privacy and Human Rights: an International Survey of Privacy Laws and Developments" (2005) EPIC; Tim Wu, "The Master Switch: the Rise and fall of Information Empires" (2010), Alfred A. Knopf; Ian Brown (ed), "Research Handbook on Governance of the Internet" (2013), Oxford University Press; Constantin Goschler et. al. (eds), "Intelligence Agencies, Technology and Knowledge Production" (2022), Taylor & Francis.

⁸ Statutory Report, page 14.



safeguards in part 7 do not account for the way that data and its availability has evolved since the Act passed.”⁹ The proposition that the exponential increase in the use of, complexity and changing nature of data was not foreseen in the period prior to, and between 2013 and 2016 is not supported by the evidence showing Parliaments and the governments’ actual knowledge during that period. Nor is it supported by the state of scientific and general public knowledge during that period.

2.1.4.1. By way of example, in 2014, the House of Commons Science and Technology Committee published a report on “Responsible use of data”,¹⁰ addressing questions such as the government’s use of “real-time big data research” and acknowledging that modern society was, and would continue to, generate an “ever-increasing” volume of data.¹¹ In 2015, the Committee undertook a second inquiry into “big data”,¹² which explicitly cited the prediction that “the total amount of global data is predicted to grow 40% year on year for the next decade.”¹³ Notably, in 2014, the Information Commissioner’s Office published a detailed paper titled “Big data and data protection”, highlighting how “high volume, high-velocity and high-variety information assets” were being used in the private and public sector,¹⁴ and detailing the applicable regulatory framework. Within that same period, the European Union’s overhaul of data protection legislation – drafting and debating the General Data Protection Regulations 2018 – was ongoing, during which time a huge amount of research was produced around the future of big data.

2.1.5. The Statutory Report further suggests that the IPA did not foresee “the extent to which cloud and commercially available tools would make powerful analysis of datasets possible.” Once again, this is not borne out by the factual evidence. A 2015 transcript of oral evidence given during the House of Commons Science and Technology Committee’s inquiry into technology issues

⁹ *ibid.*

¹⁰ House of Commons Science and Technology Committee, “*Responsible use of data*”, printed on 19 November 2014, available online: <https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/24502.htm>

¹¹ *ibid.*

¹² House of Commons Science and Technology Committee, “*The big data dilemma*”, Fourth Report of Session 2015–2016, printed on 10 February 2016, available online: <https://publications.parliament.uk/pa/cm201516/cmselect/cmsctech/468/468.pdf>

¹³ *ibid.*

¹⁴ Information Commissioner’s Office, “*Big data and data protection*”, 28 July 2014, available online: <https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220>

related to the Investigatory Powers Bill specifically dealt with issues related to cloud computing.¹⁵ Further, the report mentioned above, titled “the Big Data Dilemma” clearly articulated an understanding of advancements in computer processing that would shape the future.¹⁶ Between 2011 and 2016, the UK Government invested over £520 million in developing the UK’s big data and high-performance computing capital infrastructure.¹⁷ Notably, Amazon Web Services – the most widely used cloud computing system in the world – began offering its cloud-based computing services to business and companies as early as 2006.¹⁸

2.1.6. The Statutory Report does not present any evidence that the existing safeguards around the UKIC’s acquisition, use and retention of BPDs “do not account for the way that data and its availability has evolved since the Act passed.”¹⁹

2.2. Are the current BPD safeguards disproportionate and therefore, in need of reform?

2.2.1. PI maintains that the power to obtain BPDs under part 7 of the IPA constitutes a disproportionate and unlawful interference with the fundamental right to privacy as protected by Article 8 of the European Convention of Human Rights (ECHR) and the Human Rights Act 1998 (HRA). The acquisition, retention, and use of large databases of information plainly amounts to a serious interference with the Article 8 right to privacy.²⁰ In order for such interference to be lawful under domestic and human rights law, powers contained in part 7 must comply with the principles of legality, necessity, and proportionality. We have consistently argued that the power to obtain and retain BPDs, as provided for under part 7 do not comply with these principles.²¹

¹⁵ House of Commons Science and Technology Committee, Oral Evidence: Investigatory Powers Bill: technology issues, HC 573, 10 November 2015, available online: <https://committees.parliament.uk/oralevidence/4918/pdf/>

¹⁶ see n12.

¹⁷ *Ibid* at page 17.

¹⁸ Amazon Web Services, “What is AWS”, webpage: <https://aws.amazon.com/about-aws/>; For more detailed explanations of the broad technical systems which are part of “cloud computing” see, Antonio Regalado, “Who Coined ‘Cloud Computing?’” MIT Technology Review, 31 October 2011, available online:

<https://www.technologyreview.com/2011/10/31/257406/who-coined-cloud-computing/>; see also, Maximiliano Destefani Neto, “A brief history of cloud computing”, IBM Industry Blog, 13 August 2016, available online:

<https://www.ibm.com/blogs/cloud-computing/2016/08/23/a-brief-history-of-cloud-computing-2/>

¹⁹ Statutory Report, page 14.

²⁰ *S & Marper v UK* (2008) ECHR 1581 at §§70–76.

²¹ See, for example our case, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others* [IPT/15/110/CH](https://www.privacyinternational.org/cases/ipt/15/110/CH), in which PI challenged the powers governing the acquisition of BPD prior the IPA coming into effect. We

2.2.2. The Statutory Report suggests that “the BPD safeguards are disproportionate for some types of data, creating a negative impact on operational agility, whilst also harming capability development.”²² Notably, the Report does not explain (1) which types of personal datasets should have different safeguards applying to them and (2) which safeguards contained in the IPA are disproportionate.

2.2.3. PI strongly opposes any proposal to weaken, amend or remove the already minimal safeguards which apply to the UKIC’s powers to acquire, use, and retain any kind of BPD. Any diminution of safeguards around the acquisition and handling of BPDs would cause irreparable harm to millions of people’s fundamental right to privacy and would create unchecked opportunities for government agents to abuse their powers. Our position is supported below by two key submissions: firstly, we rely on factual evidence uncovered through litigation which illustrates that, for years, MI5 unlawfully failed to apply mandatory safeguards around the retention of bulk data to millions of people’s personal data. This evidence demonstrates that the *existing* safeguards are already failing to protect fundamental rights and prevent unlawful handling of data. Secondly, as a matter of domestic and human rights law, the fundamental principle of the rule of law requires that robust, effective, and transparent safeguards are included in any legal framework which enables interferences with fundamental rights generally and the right to privacy specifically. This ensures that powerful government agencies with wide, sweeping powers can be held accountable. It is a fundamentally basic and necessary feature of democratic governance for there to be rules which prevent arbitrary and abusive exercises of power by government agencies.

Evidence from Liberty/PI v MI5 and SSHD case (safeguards)

maintain that part 7 regime is not a substantial improvement upon the previous position, especially with regard to the disproportionate nature of the acquisition; See also, Privacy International Submission to the Joint Committee on the Draft Investigatory Powers Bill, 21 December 2015, available online: https://privacyinternational.org/sites/default/files/2017-12/Submission_IPB_Joint_Committee.pdf; See also Privacy International and Open Rights Group Submission to the Joint Committee on Human Rights on the Draft Investigatory Powers Bill, 7 Dec. 2015, para. 9 available at: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/legislative-scrutiny-draft-investigatory-powers-bill/written/25654.pdf>

²² Statutory Report, page 14.

2.2.4. As a preliminary point, we are aware that our co-complainant in *Liberty and Privacy International v the Security Service and Secretary of State for the Home Department*,²³ (the “Liberty/PI v MI5 and SSHD Case”) (Liberty) will also submit comments to the Reviewer. We have seen Liberty’s comments, which focus on the lessons learnt from the *Liberty/PI v MI5 and SSHD* case. To avoid repeating the full arguments made by Liberty, PI endorses and reiterates Liberty’s submissions at paragraphs 10 – 20. We outline below further points which are relevant to our submissions.

2.2.5. On 30 January 2023, the Investigatory Powers Tribunal (IPT) held that MI5 acted unlawfully by knowingly holding and handling people’s personal data in systems that were in breach legal requirements. Specifically, the Tribunal held that “from late 2014, there were serious failings in compliance with review, retention and deletion policies which required urgent action to be taken by the Management Board of MI5” (§§66, 79, and 160). Despite knowing about issues with non-compliance, at the most senior level, MI5 made a positive decision not to report its non-compliance to oversight bodies (§§82, 135, and 147).

2.2.6. MI5’s failure to disclose its non-compliance in the course of previous litigation amounted to a breach of its duty of candour. As a result, PI was given permission to make submissions to apply for re-opening in a previous case which challenged the lawfulness of UK intelligence agencies’ bulk surveillance powers.²⁴

2.2.7. The IPT also held that the warrants, authorisations, and directions which had been issued by the SSHD permitting MI5 to obtain personal data and process it in the non-compliant “technical environments” between late 2014 and April 2019 were unlawful. The warrants did not meet the safeguarding requirements imposed by the applicable legislation (that is the Regulation of Investigatory Powers Act 2000 (RIPA) and the IPA). This was the result of MI5’s unlawful conduct and, at least from 2016, the Secretary of State’s failure to make adequate enquiries “as to whether the statutory safeguards...were being met”

²³ [2023] UKIPTribI IPT/20/01/CH.

²⁴ *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others* IPT/15/110/CH. Submissions to re-open the case were filed at the end of February 2023.

(§§125-126). Additionally, and relatedly, in its role as an oversight body, the SSHD failed to make adequate enquiries as to the longstanding compliance risks which had been reported to the Home Office on several occasions (§107).

2.2.8. Given that the warrants that MI5 used to interfere with people's right to privacy and collect personal and sensitive data were unlawful, MI5's surveillance activities were not undertaken "in accordance with the law" therefore, in breach of the right to privacy under Article 8 of the ECHR (§§138-139).

2.2.9. PI notes with disappointment that the Statutory Report makes no mention of the IPT's significant findings from the *PI and Liberty v MI5 and SSHD* case. To be clear: one of the key oversight mechanisms (the IPT) which enables individuals and organisations impacted by the exercise of investigatory powers made an unprecedented finding about the Home Secretary's unlawful failures to make adequate enquiries as to the scale and nature of MI5's unlawful retention of data. Instead of accepting responsibility for this failing, the Statutory Report selectively says, "[s]ince the Act came into force, public authorities have developed a good working practice in applying the safeguards and associated thresholds. The IPC has separately corroborated this assessment, commenting on "the strong culture of compliance seen by my inspectors on their visits."²⁵

2.2.10. The Statutory Report deliberately fails to highlight a separate finding from 2019 by the then-Investigatory Powers Commissioner, Fulford LJ – which stated: "MI5 has inadequate control over where data is stored; [REDACTED]; and the deletion processes which applied to it. Two specific aspects of the. [TE] exemplify the undoubted unlawful manner in which the data has been held and handled." Fulford LJ makes it clear that "MI5's use of warranted data in [TE] [was], in effect, in "special measures" and the historical lack of compliance with the law is of such gravity that IPCO will need to be satisfied to a greater degree than usual that it is "fit for purpose."²⁶

²⁵ Statutory Report, page 11.

²⁶ To access this report, please see the 'Legal Files' section of the Privacy International's case page "[MI5 Ungoverned Spaces Challenge](#)" and click on "[IPCs Decision 5 April 2019](#)".

2.2.11. The facts which emerged in the course of the Liberty/PI v MI5 and SSHD case demonstrate that even the existing safeguards around bulk data acquisition and retention were not effective in practice. It is important to highlight that the unlawfulness was not a 'one-off error', but as we argued in the proceedings, "a protracted systemic and systematic failure"²⁷ on multiple levels:

2.2.11.1. First, in the handling of data by MI5. Not only did the individuals and bodies responsible for oversight allow unlawful retention of data to persist for years, but additionally facilitated *more* unlawfulness by continuing to allow bulk data to be ingested into deficient systems;

2.2.11.2. Second, in the outputs of MI5, whether in terms of candour in warrantry (to the SSHD and the Judicial Commissioners) or candour in legal proceedings, the agency unlawfully failed to disclose its non-compliance.

Rule of law and human rights

2.2.12. The mere existence of personal datasets held in bulk by law enforcement and intelligence agencies amounts to an interference with *millions* of peoples' Article 8 rights. As noted previously, PI maintains that such general and indiscriminate acquisition of data cannot be "necessary in a democratic society" (Article 8(2)). If it is to be pursued, nonetheless, the interference will be unlawful unless undertaken "in accordance with the law" (Article 8(2)). In order for an interference to meet the requirement of lawfulness, the law must contain an effective "measure of legal protection against arbitrary interferences by public authorities."²⁸ The case law of the ECtHR is clear that the minimum safeguards that should be set out in law in order to avoid abuses of power include a definition of the categories of the people liable to have their data recorded and retained; a limit on the duration of the retention; the procedure to be followed for examining, using and storing the data obtained;

²⁷ To access the Claimant's Skeleton Argument in the Liberty/PI v MI5 and SSHD, please see the 'Legal Files' section of the Privacy International's case page "[MI5 Ungoverned Spaces Challenge](#)" and click on "[Claimant's Skeleton for Substantive Hearing 25-29 July 2022](#)".

²⁸ *Gillan v United Kingdom* (2010) 50 EHRR 45 at §76-77.

the precautions to be taken when communicating the data to other parties; and the circumstances in which the data may or must be erased.²⁹

2.2.13. Any proposed diminution of existing safeguards around the acquisition and use of BPDs would weaken the already minimal protections of our right to privacy that the Act contains, without equivocally providing any benefit to the UKIC's intelligence gathering capabilities.

2.2.14. The existing definition of BPDs under s.199 of the IPA is extremely broad, covering any "(a) set of information that includes personal data relating to a number of individuals [and] (b) the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence services in the exercise of its functions." In the course of litigation brought by PI against a number of intelligence agencies and the Secretary of State for the Home Department,³⁰ an MI5 witness acknowledged that the agency held the following categories of BPD: law enforcement and intelligence, travel datasets (including biometric information which is contained in passport information and travel activity held in bulk), communications datasets, finance datasets, identification and population datasets and commercial datasets (which provide details of individuals involved in commercial activities).³¹

2.2.15. Within this context which explains the massive range of personal datasets which may already be acquired and retained – in bulk – by law enforcement and intelligence agencies in the UK, it is difficult, if not impossible to conceive of any specific types of personal datasets which could be removed from the ambit of the safeguards contained in part 7 of the IPA while still providing any level of protection for people's right to privacy.

2.2.16. We would remind the Reviewer that, the Intelligence and Security Committee's 2015 Report revealed that in the period prior to avowal of the agencies' use of bulk surveillance powers, there had been abuse of BPDs by

²⁹ See *Malone v UK* (1985) 7 EHRR 14 at §67 and §99; *Huvig v France* (1990) 12 EHRR 528 at §29; *Rotaru v Romania* (App No. 28341/95, 4 May 2000) at §55.

³⁰ *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communication Headquarters, Security Service, Secret Intelligence Service* [2016] UKIPTrib 15_110-CH

³¹ To access this witness statement, please see the 'Legal Files' section of the Privacy International's case page "Bulk Personal Datasets & Bulk Communications Data challenge" and click on "[Amended w/s GCHQ 08.07.2016, Amended w/s MI5 11.07.2016, Amended w/s SIS 11.07.2016](#)" (MI5 witness statement begins on page 35).



the staff of all of the three Agencies, and each of the three intelligence agencies “had disciplined – or in some cases – dismissed staff for inappropriately accessing personal information held in these datasets for years.”³² Notably, no prosecutions appear to have been brought as a result of this unlawful conduct. More importantly, it is not clear whether the victims of the conduct were ever notified of the wrongful access or compensated for the harm they will have suffered.

2.2.17. The ability to access any large database or aggregation of data about innocent people without a warrant will inevitably lead to abuse. All types of personal datasets which are acquired by law enforcement and intelligence agencies and held in bulk must be protected by robust, effective, and transparent safeguards.

2.3. Do the current BPD safeguards “inhibit the UKIC’s ability to maximise the benefits of digital transformation?”³³

2.3.1. The Statutory Report suggests that the IPA has “limitations” which are inhibiting the UKIC’s ability to maximise the benefits of digital transformation, and which will require legislative change. While we have already provided, at paragraphs 2.1 and 2.2 of these comments, our response to the suggestions that the BPD safeguards are “disproportionate for some types of data”, it is also significant to highlight that the IPA does not impose any limits or restrictions on the types of surveillance technologies and equipment that law enforcement and intelligence agencies are able to acquire, develop and deploy covertly. PI submits that the existing powers under the IPA (as well as related legislation) has enabled law enforcement and intelligence agencies to acquire an ever-expanding range of surveillance and intelligence gathering technologies, in order to maximise their capacities in the context of “digital transformation”. Contrary to the position put forward in the Statutory Report, the constant expansion of UKIC’s surveillance capabilities points to a need for more robust safeguards, not less.

³² Intelligence and Security Committee of Parliament, “Privacy and Security: A modern and transparent legal framework”, March 2015, at para. 163, available online: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf

³³ Statutory Report, page 14.

2.3.1.1. One example of highly intrusive, indiscriminate, and covert surveillance technology which police forces around the UK are thought³⁴ to have acquired and deployed in various public spaces – including at protests – are IMSI catchers (International Mobile Subscriber Identity catchers). IMSI catchers can be covertly used to locate and track all mobile phones that are switched on in a certain area. They do this by mimicking a cell-tower and ‘enticing’ all mobile phones within their range to connect to them. IMSI catchers can force those mobile phones to transmit and reveal the phone user’s personal details without the user’s knowledge. Some IMSI catchers can be used to ‘intercept’ text messages, calls and internet traffic, allowing whoever is operating the IMSI catcher to read or listen to personal communications. Some IMSI catchers can even re-route or edit communications and data sent to and from our phone and can be used to block service so that phones can no longer be used.³⁵

2.3.1.2. In 2016, PI submitted freedom of information requests to a number of police forces seeking records related to UK police forces’ purchase and use of IMSI catchers.³⁶ The policing bodies refused PI’s requests on the grounds that they could “neither confirm nor deny” whether they held information responsive to the request, primarily relying on the national security exemption contained in s.24(2) of the Freedom of Information Act. In the course of our appeal to the Information Rights Tribunal,³⁷ the head of the Technical Surveillance Unit within the Metropolitan Police gave evidence which justified this lack of transparency on the grounds that maintaining secrecy of covert technology utilised by police prevents “criminal networks and terrorists from building up an accurate picture”³⁸

³⁴ While police forces across the UK have never confirmed or denied whether they have acquired IMSI catchers, a substantial amount of information in the public domain underpins the widespread understanding that police forces across the UK have acquired and deployed IMIS catchers in public spaces. For more detail on this, see “Witness Statement by Ailidh Callander”, 18 April 2019, submitted as evidence in *PI v the Information Commissioner’s Office*, the Commissioner of the Metropolitan Police and the Police and Crime Commissioner for Wawrickshire, available online: <https://privacyinternational.org/sites/default/files/2019-09/Ailidh%20Callander%20Witness%20Statement%20-%20redacted.pdf>

³⁵ Privacy International, “IMSI Catchers: PI’s Legal Analysis”, June 2020, available online: <https://privacyinternational.org/report/3965/imsi-catchers-pis-legal-analysis>

³⁶ Privacy International, “*PI v Information Commissioner’s Office* EA/2018/0164/0172”, webpage:

<https://privacyinternational.org/legal-action/privacy-international-v-information-commissioners-office-imsi-catcher-foia>

³⁷ *PI v Information Commissioner’s Office* EA/2018/0164/0172, First Tier Tribunal (Information Rights), available online: [https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2576/Privacy%20International%20EA.2018.0164%20\(18.02.20\).pdfv](https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2576/Privacy%20International%20EA.2018.0164%20(18.02.20).pdfv)

³⁸ n37, *PI v Information Commissioner’s Office* at para 27.

of the police's capabilities. The decision to neither confirm nor deny was further justified on the basis that "the deployment of any covert technique or technology is subject to multiple checks and balances to ensure that the rights of the citizenry are protected."³⁹

2.3.1.3. This example illustrates that: (a) contrary to the submissions in the Statutory Report, law enforcement agencies continue to acquire highly intrusive surveillance technologies which allows them to collect huge amounts of digital information, without limitation; and that (b) law enforcement agencies can even keep the use of these technologies secret by relying on the existence of robust legal safeguards and 'checks and balances'. We note, of course, that depending on their implementation, the use of IMSI catchers would be considered interception, communications data acquisition or equipment interference under the IPA and would therefore be governed by parts 2, 4 or 5 of the IPA instead of Part 7. Nevertheless, we rely on IMSI catchers by way of analogy because it is extremely difficult to obtain actual knowledge about the technology that is being deployed to obtain BPDs. Additionally, BPDs can lawfully be obtained and retained under s.201 of the IPA through other lawful warrants (like those granted under parts 2-4 of the IPA).

2.3.2. The point is that law enforcement agencies develop, acquire, and deploy technologies which have seemingly limitless surveillance capabilities. They are able to do this in secret and avoid public scrutiny under the current legal regime. In order to justify this level of secrecy and lack of accountability, they rely on the fact that there are, at law 'checks and balances' – including the safeguards contained in the IPA – which prevent abuse. Weakening those safeguards is not justifiable within the current context.

2.3.3. More broadly, PI has undertaken in-depth research into a range of surveillance technologies that we have confirmed have been used by law enforcement and intelligence agencies in the UK for covert surveillance in line with the powers contained in the IPA: this includes, but is not limited to [social media intelligence gathering](#), [live and static facial recognition technology](#),

³⁹ *ibid.*

drones (or unmanned aerial vehicles), used by both [police](#) and the [UK's immigration authorities](#), [mobile phone extraction technology](#) and [computer network exploitation](#) (which includes hacking and breaking end-to-end encryption). Notably, this is only the technology we know about. There is, of course a broad range of surveillance technology which is widely available to governments, and a can reasonably expected to be used by the UKIC, including [zero-click hacking spyware](#).

3. Omission of BCD from the Review

3.1. While the ToR do not explicitly include any references to the power to obtain bulk communications data within the IPA, PI briefly points out that the powers contained in part 6 similarly suffer from legal defects that we highlighted in relation to part 7. The issues arising out of part 6 should be considered as part of any review of the IPA. In PI's challenge to a previous iteration of the power to obtain bulk acquisition of communications data,⁴⁰ the Court of Justice of the European Union held that "general and indiscriminate" acquisition of communications data by the UKIC violates EU law.⁴¹ The IPA is identical to this earlier power in permitting general and indiscriminate acquisition. PI thus endorses Liberty's arguments, as presented in its ongoing challenge against the IPA, that Part 6, Chapter 2 is incompatible with EU law.⁴²

4. Ways to increase resilience and agility of the oversight regime in light of the experience of the last five years of operation.

4.1. The ToR make it clear that the review is seeking to consider whether amendments to the role of the IPC and wider oversight regime are required to ensure flexibility and resilience. We are concerned that, in the Statutory Report, the SSHD is framing the need for greater flexibility and resilience as a basis for weakening the powers of the oversight bodies.

4.2. PI submits that the evidence which was disclosed in the Liberty/PI v MI5 and SSHD case, as well as the IPT's final conclusions illustrate that the current oversight

⁴⁰ Privacy International, "*CJEU Bulk Challenge*", webpage: <https://privacyinternational.org/legal-action/cjeu-bulk-challenge>

⁴¹ CJEU C/623/17.

⁴² Liberty, "*Legal Challenge: Investigatory Powers Act*", webpage: <https://www.libertyhumanrights.org.uk/issue/legal-challenge-investigatory-powers-act/>

mechanisms, should in fact, be strengthened. Every agency and government body which is empowered, under the IPA, to undertake covert surveillance utilise bulk powers or gain access to personal datasets in bulk, must be subjected proactive oversight and monitoring by independent bodies. The oversight mechanisms which are currently relied on under the IPA are ineffective at an operational level and must be improved. We have set out below three sections which support this position: firstly, we contextualise the need for robust oversight where huge amounts of data are being handled, secondly, we include specific evidence from the Liberty/PI v MI5 and SSHD case which relate to oversight failures, and finally, we outline the relevant principles established under international human rights law in this context.

4.3. Contextualising the extent of the 'Information Management' systems that the oversight regime relates to

4.3.1. PI notes that the Investigatory Powers Commissioner (IPC), the appointed Judicial Commissioners, the Investigatory Powers Commissioner's Office (IPCO) and the Office for Communications Data Authorisations (OCDA) oversee the exercise of powers under the IPA, and specifically the use of covert investigatory powers. This includes oversight of more than 600 public authorities which are empowered to use covert investigatory powers.

4.3.2. Information management is critical to making any intelligence gathered by law enforcement and intelligence agencies useful and actionable. The IPC and IPCO both play a critical role in overseeing the functionality of each agencies' information management systems and practices, including their operational efficacy and their compliance with IPA safeguards and statutory and non-statutory codes and guidance.

4.3.3. The UKIC and agencies have repeatedly argued that "bulk collection of personal data sets and communications data is needed to 'make links'... and discover threats, as opposed to only using targeted tools on known threats, often described as "needing the haystack in order to find the needle."⁴³

⁴³ n32 at page 4 and page 25.

- 4.3.4. Information management on such huge scales can be incredibly complex, and it would be irresponsible to assume that agencies are 'getting it right' without appropriate audit mechanisms by oversight bodies. PI submits that, where more than 600 government agencies are empowered to gather and retain vast amounts of data, meaningful and full-access oversight is operationally necessary.
- 4.3.5. Intelligence agencies must be accountable for the decisions they make – both in terms of data collection and data analysis and management. This point was highlighted in Volume 3 of the Manchester Arena Inquiry,⁴⁴ where the Chair made it clear that it is always sufficient "to simply rely on internal reviews conducted by the Security Service...with the only evidence of those reviews and their conclusions coming from corporate representatives."⁴⁵
- 4.3.6. The point is further strengthened by the fact that in two separate cases which PI brought challenging intelligence agencies' exercises of power, the agencies' corporate witnesses gave inaccurate and incorrect evidence to the IPT which then had to be corrected. Firstly, in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others*,⁴⁶ the corporate witness for GCHQ gave inaccurate evidence about the delegation of powers from the relevant Secretary of State to GCHQ, which led to the IPT overturning parts of its initial judgment.⁴⁷ Second, in the *Liberty/PI v MI5 and the SSHD*⁴⁸ an MI5 witness who was described as "the Director responsible for information, compliance, security, communications, strategic policy and international liaison in MI5"⁴⁹ inaccurately represented MI5's internal processes for notifying errors to IPCO. We only know that this was incorrect because it was corrected by another MI5 witness who stated "I am unsure how this inaccuracy...came to appear" in their witness statement.⁵⁰

⁴⁴ Manchester Arena Inquiry, Volume 3: Radicalisation and Preventability, HC 1137, March 2023, available online: <https://files.manchesterarenainquiry.org.uk/reports/2023/MAI-Final-PDF-Volume-3.pdf>

⁴⁵ *ibid* at Page iii

⁴⁶ IPT/15/110/CH

⁴⁷ See the judgement of 23 July 2018 in IPT/15/110/CH (the second judgement).

⁴⁸ [2023] UKIPTribl IPT/20/01/CH.

⁴⁹ Third Witness Statement of Witness A; made public during OPEN oral proceedings in *Liberty and Privacy International v the Security Service and Secretary of State for the Home Department* [2023] UKIPTribl IPT/20/01/CH. PI can provide the Reviewer with a copy upon request.

⁵⁰ First Witness Statement of Witness C; made public during OPEN oral proceedings in *Liberty and Privacy International v the Security Service and Secretary of State for the Home Department* [2023] UKIPTribl IPT/20/01/CH. PI can provide the Reviewer with a copy upon request.

4.4. Evidence from Liberty/PI v MI5 and SSHD case (oversight)

- 4.4.1. As outlined at paragraph 2.2.7, the IPT’s recent ruling in the Liberty/PI v MI5 and SSHD case deal directly with issues related to the SSHD’s oversight over MI5’s compliance with safeguards which are pre-conditions to obtaining warrants for covert surveillance. PI submits that the IPT’s findings that the SSHD failed to make adequate inquiries into the scope and nature of non-compliance highlights that the current oversight regime has led to systematic failures in accountability.
- 4.4.2. The prescribed internal and external oversight systems failed to uncover ‘root and branch’ failures for at least seven years. The oversight mechanisms in place proved inadequate in practice to prevent and/or rectify these breaches. The system was overwhelmingly reliant on MI5’s own assessment of its systems, and the importance (or lack of it) that MI5 decided to accord to the legality of its data handling. Neither internal lawyers nor the SSHD provided any meaningful independent oversight over the process, in circumstances where the Secretary of State was content to trust the limited information being shared with him or her by MI5. As a result, MI5 was able to conceal systemic deficiencies from successive IPCs.⁵¹
- 4.4.3. Notably, in the Liberty/PI v MI5 and SSHD case, the IPT made it clear that, in relation to the persistent failures related to the application of legal safeguards to certain data holdings, MI5 had a duty to provide “full and frank disclosure” to the SSHD when applying for warrants to carry out surveillance activities which require warrants or authorisation (§134-135).
- 4.4.4. It is important to highlight that the double-lock process within the IPA requires the duty of candour of the intelligence agencies and government to proactively inform the Commissioners of any relevant considerations or issues when they conduct the review of a Secretary of State’s decision to approve a warrant.⁵²

⁵¹ For more detailed arguments on this point, please see the ‘Legal Files’ section of the Privacy International’s case page “[MI5 Ungoverned Spaces Challenge](#)” and click on “[Claimant’s Skeleton for Substantive Hearing 25-29 July 2022](#)”.

⁵² See: <https://www.ipco.org.uk/what-we-do/the-double-lock/>

4.4.5. PI has continuously raised concerns with the process and the powers of the Judicial Commissioners. PI maintains that Commissioners should have the power to fully and completely assess whether a warrant is necessary and proportionate. The Codes of Practice refer to the Commissioner's review of the Secretary of State's conclusions rather than a full and complete assessment of the warrant.⁵³ Therefore, there are significant limitations on the scrutiny the Judicial Commissioners will exercise.

4.4.6. PI submits that these failings amount to a systemic failure in the statutory oversight process. As such, the existing oversight regime is incompatible with the right to privacy under Article 8.⁵⁴

4.5. Human Rights Principles

4.5.1. The Office of the United Nations High Commissioner for Human Rights presented a report on the serious human rights implications that mass surveillance programmes have in the context of the International Covenant on Civil and Political Rights (ICCPR). The Report stressed the need to have an effective oversight process over surveillance programmes, a combination of administrative, judicial, and parliamentary oversight mechanisms that are truly impartial, independent, and transparent.⁵⁵

4.5.2. Further, the Council of Europe's Commissioner for Human Rights has previously made clear that in order to establish effective oversight regimes, "states should establish or designate one or more bodies that are fully independent from the executive and the security services to oversee all aspects of security service regulations, polices, operations, [and] data collection and administration."⁵⁶ In the same report, the Commissioner emphasised that, "independent ex ante authorisation should be extended to:

⁵³ For more detailed arguments on this point, please see Privacy International's Submission to the Home Office Investigatory Powers Act 2016 Consultation on the Draft Codes of Practice <https://privacyinternational.org/sites/default/files/2017-12/Privacy%20International%20-%20Response%20to%20Consultation%20on%20IPA%20Codes%20of%20Practice%20-%20April%202017.pdf>

⁵⁴ *Zakhrov v Russia* (App No 47143/06) [2015] GC.

⁵⁵ Report of the Office of the United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age', 30 June 2014, available online: <https://documents-dds-ny.un.org/doc/UNDQC/GEN/G14/088/54/PDF/G1408854.pdf?OpenElement>

⁵⁶ Council of Europe Commissioner for Human Rights, "Issue paper: Democratic and Effective Oversight of National Security Services, at page 11, (5 June 2015) available online: <https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb>



untargeted bulk collection of information; the collection of, and access to communications data (including when held by the private sector); and potentially computer network exploitation. The process by which intrusive measures are authorised and re-authorised should itself be subject to scrutiny.”⁵⁷

4.5.3. The UN Special Rapporteur on the Right to Privacy also expressed concerns with the double-lock process. The rapporteur stated that “the residual concern that I have expressed with various UK authorities lies with those parts of the IPA 2016 which impose on IPCO the dual tasks of both authorising surveillance and then providing oversight of the way that the very same surveillance is carried out. To many observers, and especially people sitting outside the British Isles, this arrangement still smacks of the new UK law creating a position where somebody is expected to be marking his own homework.”⁵⁸ The Rapporteur stated that “the system of having politicians involved in signing off on warrants of interception remains inherently open to abuse if a conflict of interest should arise as to whom it is being proposed be put under surveillance”.⁵⁹

4.5.4. In the European Court of Human Rights case of *Big Brother Watch and Others v the United Kingdom*,⁶⁰ at § 349 and §356, the Grand Chamber highlighted:

“In the context of bulk interception, the importance of supervision and review will be amplified because of the inherent risk of abuse and because the legitimate need for secrecy will inevitable mean that, for reasons of national security, States will often not be at liberty to disclosure information concerning the operation of the impugned regime.

[...]

Each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection bearers, the choice and application of the selectors and query terms, and the use, storage, onward

⁵⁷ *Ibid.*

⁵⁸ End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland. Available at: <https://www.ohchr.org/en/statements/2018/06/end-mission-statement-special-rapporteur-right-privacy-conclusion-his-mission>

⁵⁹ *Ibid.*

⁶⁰ Apps Nos. 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, European Court of Human Rights (25 May 2021).

transmission, and deletion of the intercept material – should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the “interference” to what is “necessary in a democratic society.”

4.6. The operation of the UK’s national security policies must not be shielded from detailed and robust scrutiny. “Agility” should not come at the cost of effective oversight, particularly when agencies are dealing with huge amounts of data, which they have repeatedly, and openly, admitted are incredibly difficult to manage. Most notably, from our Liberty/PI v MI5 and SSH case, creating situations where the agencies themselves have a “limited understanding of what is on [their] systems.”⁶¹

5. General comments on the consultation process

5.1. The Secretary of State for the Home Department (SSHD) was under a statutory obligation to prepare a report on the operation of the IPA (s.260 IPA). This report was published in February 2023. A wide range of intelligence agencies, policing bodies and government agencies contributed to that report.⁶²

5.2. The Review, and the appointment of the Reviewer was made public on the 17 January 2023, and set to be completed within three months. The relevant consultation period effectively ran from 9 February 2023 to 10 March 2023, with important supplemental information being provided on 17 February 2023.

5.3. This led to an unacceptably short consultation period for stakeholders to submit evidence to the Review, which has undoubtedly negatively impacted the general public’s only opportunity to provide comprehensive and meaningful comments on the operation of the IPA over the past five (5) years.

5.4. PI wishes to remind the government of the Consultation Principles 2018,⁶³ which it previously committed to. The guidance on these Consultation Principles clearly provides that the timeframe for consultation should be proportionate and realistic

⁶¹ See for example, a minute produced by MI5 in 2016 [https://privacyinternational.org/sites/default/files/2023-01/04.%20Minute%20\(MI5%20Core%20Doc%2015\)%20-%20C2_58.pdf](https://privacyinternational.org/sites/default/files/2023-01/04.%20Minute%20(MI5%20Core%20Doc%2015)%20-%20C2_58.pdf)

⁶² Statutory Report, page 1.

⁶³ ‘Consultation Principles 2018’. Available at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/691383/Consultation_Principles_1.pdf

to allow stakeholders sufficient time to provide a considered response.⁶⁴ Furthermore, the capacity of the groups being consulted to respond should be taken into consideration, and specifically in relation to contentious policies, a longer timeframe should be considered.⁶⁵ Although, the revised Code does not refer to a specific timeframe, we remind the government that previously it was 12 weeks.

5.5. Members of the public and advocacy groups have played a crucial role in uncovering important information about the breaches of the IPA over the past 5 years, and many have been directly impacted by the powers contained in the IPA and/or predecessor legislation.⁶⁶ Members of the public must play a role in informing public understanding about (and confidence in) the use of these important powers.⁶⁷ This is particularly important in light of the fact that law enforcement agencies, intelligence agencies and other government agencies have already been given the opportunity to contribute to the SSHD's report. Individuals, civil society, and the wider public stand to lose the most if the safeguards and oversight regime within the IPA are reformed or weakened.

5.6. Finally, PI is concerned that the Home Secretary's Statutory Report appears to have set the scope of the review. The topics being considered by Lord Anderson's review, as outlined in the terms of reference, narrowly reflect those topics highlighted in the government's report. This has meant that several other topics and issues with the IPA appear to be out of scope of this review for example, bulk communications data.

6. Conclusions and Recommendations

6.1. PI does not consider that, in the period between 2016 and 2023, there has been an emergence of technological change which has made the safeguards around BPD

⁶⁴ 'Consultation Principles: Guidance'. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/255180/Consultation-Principles-Oct-2013.pdf

⁶⁵ *ibid.*

⁶⁶ See, for example, Human Rights Watch, "UK: Human Rights Watch Challenges Surveillance" webpage: <https://www.hrw.org/news/2015/09/14/uk-human-rights-watch-challenges-surveillance>; Privacy International, "UK intelligence agency admits unlawfully spying on Privacy International", 25 September 2018, available online: <https://privacyinternational.org/press-release/2283/press-release-uk-intelligence-agency-admits-unlawfully-spying-privacy>

⁶⁷ SSHD specifically says that the review process is key to ensuring "The effective operation of the act ensures that there is appropriate oversight in place to give the public confidence in the use of these important powers;" <https://www.gov.uk/government/news/lord-anderson-appointed-to-review-the-investigatory-powers-act#full-publication-update-history>

in part 7 “disproportionate”. The acquisition and use of BPDs must be regulated in accordance with the minimum safeguards under domestic and international human rights law. The principles underpinning the substance of ‘adequate safeguards’ is well-established in human rights law.⁶⁸ Properly implemented, these safeguards are necessary for the protection of the rights to privacy, freedom of expression, freedom of assembly and the right to an effective remedy.

6.2. The acquisition and use of BPDs is not less intrusive than the acquisition and use of communications data or intercept material. BPDs obtained from corporate entities – such as email providers, banks, social media applications, and operators of ‘smart devices’ – inevitably include information about millions of people (who are unlikely to be of any intelligence interest), who have a reasonable expectation of privacy in that data. PI’s detailed submissions to the Home Office’s consultation on the (then) draft codes of practice⁶⁹ related to the IPA further explain how the acquisition and use of BPDs must be regulated.

6.3. The current oversight regime is operationally ineffective and must be strengthened in order to prevent intelligence agencies’ unlawful handling of millions of people’s private data. Warrant authorisation and oversight should be institutionally separated,⁷⁰ and IPCO should be fully resourced to conduct audits and reviews over each agency to ensure that errors and non-compliance are not systematically ignored. The acquisition and deployment of covert surveillance technologies by law enforcement and intelligence agencies should be controlled through independent oversight. To guarantee a minimal level of transparency regarding agencies’ use of covert surveillance tools, oversight bodies must be empowered to undertake meaningful human rights impact assessments prior to the deployment of new systems and technologies.

6.4. The ‘digitisation’ of communications, production, consumption, data creation and data storage, amongst other social activities, has not occurred in a policy vacuum. Domestically and internationally, individuals, communities and organisations have

⁶⁸ See, Privacy International, “*PI’s Guide to International Law and Surveillance*”, December 2021, pp. 59-182, available online: https://privacyinternational.org/sites/default/files/2022-01/2021%20GILS%20version%203.0_0.pdf.

⁶⁹ Privacy International, “*PI’s Submission to the Home Office Investigatory Powers Act 2016 Consultation on the Draft Codes of Practice*”, April 2017, available online: <https://privacyinternational.org/sites/default/files/2017-12/Privacy%20International%20-%20Response%20to%20Consultation%20on%20IPA%20Codes%20of%20Practice%20-%20April%202017.pdf>

⁷⁰ Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29 (3 August 2018) at para 40, available online: <https://digitallibrary.un.org/record/1640588>

demanding that alongside this 'big-data boom' institutions (particularly powerful institutions such as intelligence agencies and technology giants like Google, Meta, and Apple), are subject to, and adhere to enforceable rules that are essential for the protection and maintenance of our rights, dignity, and ability to live freely.

6.5. PI hopes the Reviewer will consider the comments herewith as a counterpoint to the Statutory Report, which entirely ignores this public's concern with the exploitation of our data. The IPA already contains unprecedentedly broad powers, many of which are subject to insufficient safeguards or unlawful in their entirety. Rather than sanctioning a further weakening of those safeguards, as the Statutory Report appears to be proposing, PI encourages the Reviewer to acknowledge the notable failures in oversight of the past five years and encourage more robust safeguards which are effectively operationalised.