INDEPENDENT REVIEW OF THE INVESTIGATORY POWERS ACT 2016

by

DAVID ANDERSON

(Lord Anderson of Ipswich KBE KC)

JUNE 2023

Presented to the Prime Minister
pursuant to terms of reference
published on 9 February 2023

CONTENTS

ANNEXES

EXECUTIVE SUMMARY

- **The purpose of this independent Report is to consider some specific proposals for amending the Investigatory Powers Act 2016 (IPA), arrived at by the Home Office following its post-legislative review, so as to inform proposals for future legislation.** (Chapter 1)

- **The first and most substantial proposal is to amend IPA Part 7 by creating a new, light-touch regulatory regime for the retention and examination by the UK Intelligence Community (UKIC) of bulk personal datasets in respect of which individuals have a low or no expectation of privacy. I endorse that proposal, on condition that datasets (or datasets of a given class) be placed in the low/no category only with the approval of an independent Judicial Commissioner.** (Chapter 3)

- **The second proposal is to amend one of the three conditions in IPA s62 so as to facilitate the use of Internet Connection Records for target discovery. I endorse that objective but consider that it could be better achieved by creating a fourth condition, which would be available only to UKIC and only for national security-related and serious crime purposes.** (Chapter 4)

- **The third proposal is to amend IPA s87 so as to ensure that technological changes notwithstanding, a mechanism continues to exist whereby UK telecommunications operators may be required, if the Secretary of State and a Judicial Commissioner agree, to retain the communications data of 'inbound roamers' with foreign SIM cards. I endorse that proposal.** (Chapter 5)

- **I comment also on a number of other proposals aimed at clarifying certain definitions in the IPA and making its warrantry and oversight processes more resilient.** (Chapters 6, 7, 8 and 9)

- **The proposals that I have endorsed would leave the IPA's central mechanisms intact, including the strong independent scrutiny that is its hallmark. If enacted in the form I have recommended, they should give UKIC, law enforcement and the oversight body IPCO useful extra agility in important areas.**

- **This Report is set in the context of current developments in the threat picture and in technology (including AI), which are likely to require a wholesale replacement of the IPA for the 2030s. I conclude with some suggestions as to how this process might be started.** (Chapters 2, 10)

1. INTRODUCTION

The Investigatory Powers Act

1.1. The Investigatory Powers Act 2016 (**IPA**) sets out statutory powers used by public authorities, including law enforcement (**LE**)[1] and the UK Intelligence Community (**UKIC**),[2] to obtain communications and data about communications.[3] The Act was intended to ensure that these powers, and their attendant safeguards, were clear and understandable. It also improved processes for authorisation and oversight, notably by requiring certain categories of warrants to be approved by independent Judicial Commissioners (**JCs**), working under an Investigatory Powers Commissioner (**IPC**) whose Office (**IPCO**) provides technical and judicial oversight of how investigatory powers are used.[4]

1.2. The government Bill which became the IPA was based on principled recommendations contained in three expert reports, including my own *A Question of Trust* (**AQOT**).[5] The measures proposed were then subject to extensive pre-legislative and legislative scrutiny.[6] As part of this process, I was commissioned to evaluate the operational case for the four bulk powers now provided for in Parts 6 and 7 of the Act. The findings of that review were published as *Report of the Bulk Powers Review* (**RBPR**).[7]

---

1 LE is a collective term for the Metropolitan Police, which as well as policing London has a number of national functions including the coordination of Counter-Terrorism Policing (**CTP**); the 43 other territorial police forces in England; Police Scotland and the Police Service of Northern Ireland; the National Crime Agency (**NCA**) which leads the fight against serious and organised crime; and certain other public authorities including His Majesty's Revenue and Customs (**HMRC**).

2 UKIC is used in this Report as a collective term for the UK's three non-military security and intelligence agencies, sometimes referred to as intelligence services, Agencies or SIAs: the Security Service (**MI5**), the Secret Intelligence Service (**MI6**, also known as SIS) and the Government Communications Headquarters (**GCHQ**).

3 A full list of the acronyms used in this Report is at Annex 1.

4 The IPC's annual reports shed significant light on the operation of investigatory powers. See further the analysis of Daragh Murray and ors., *Effective Oversight of Large-Scale Surveillance Activities: A Human Rights Perspective* 11 J. Nat'l Sec Law & Policy (2021), 743-770.

5 D. Anderson Q.C., *A Question of Trust: Report of the Investigatory Powers Review*, June 2015, whose scope was limited to interception and CD but whose 125 recommendations (one of them conveyed privately to the Prime Minister) were for the most part adopted in the Bill. The other two reports were prepared by the Intelligence and Security Committee of Parliament (**ISC**), which focussed largely on UKIC (*Privacy and Security: a modern and transparent legal framework* HC 1075, March 2015) and a panel convened by the Royal United Services Institute (**RUSI**), whose recommendation of a '*double lock*', building on my own recommendation of independent judicial authorisation, was adopted as part of the IPA. (*A Democratic Licence to Operate*, July 2015).

6 Notably by a parliamentary Joint Committee on the Draft Investigatory Powers Bill, whose report of February 2016 contained 155 recommendations, most of them adopted in the Bill.

7 D. Anderson Q.C., *Report of the Bulk Powers Review*, August 2016, Cm 9326.

1.3. The IPA was welcomed by the UN's Special Rapporteur on the Right to Privacy, Professor Joe Cannataci, who at the conclusion of a visit to the UK for a detailed inspection of the arrangements for its operation, reported in 2018 that:

> 'While the new set-up may still contain a number of imperfections, the UK has now equipped itself with a legal framework and significant resources designed to protect privacy without compromising security. Given its history in the protection of civil liberties and the significant recent improvement to privacy laws and mechanisms, the UK can now justifiably reclaim its leadership role in Europe as well as globally.
>
> The UK is now co-leading with that tiny minority of EU states which have made a successful effort to update their legislative and oversight framework dealing with surveillance.'[8]

1.4. Like previous legislation in this area the IPA has been subject to intensive legal challenge from NGOs, with mixed results. The principal cases decided since 2016 are summarised in Annex 4 to this Report.

Scope of this Review

1.5. After a review undertaken by policy officials, government lawyers and representatives from across the operational community, the Home Office during 2022 prepared the post-legislative report required by IPA s260 (**the Home Office Report**). The Home Office Report was published and laid before Parliament on 9 February 2023.[9] It concluded that the IPA had largely achieved its aims, but that future substantial reform was likely to be needed in view of developing technology and the evolving requirements of protecting national security and tackling serious crime. It also concluded that certain specific changes were necessary in the short term to ensure that LE and UKIC could continue effectively to exercise their investigatory capabilities.

1.6. The main purpose of this Review is to consider the specific areas for change identified as a priority in the Home Office Report, with a view to informing proposals for future legislation. Those priority areas relate to Bulk Personal Datasets (**BPDs**), Internet Connection Records (**ICRs**), Data Retention Notices (**DRNs**), some statutory definitions, Targeted Examination Warrants (**TEWs**), the warrantry process and oversight. I was asked to give particular priority to the issue of BPDs, which forms the subject of Chapter 3.

---

8 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, June 2018.

9 Home Office, *Report on the Operation of the Investigatory Powers Act 2016*, February 2023.

1.7. Chapter 2 sets the scene by identifying some material developments in the threat picture and in technology and ways of working. Chapters 3-9 address each of the priority areas in turn. Changes not identified as immediate priorities are beyond the scope of this Report, but Chapter 10 peers cautiously into the future. My recommendations are summarised in Chapter 11.

Conduct of this Review

1.8. I was commissioned on 16 January 2023 to start work on the Review, with the budget to assemble a small Review team of my own choosing (though each of its members was required to have Developed Vetting status) and the instruction to report to the Prime Minister after three months.

1.9. The team that has assisted me throughout this process consisted of Natasha Barnes, a barrister in private practice, and John Davies, a self-employed technical consultant and a member of the IPC's Technology Advisory Panel (**TAP**).[10] Each has experience of working with UKIC but also with a wide range of other organisations and individuals. They brought not only specific expertise to the Review, but an inquiring and independent disposition. I am most grateful to both of them for their work. The views expressed in this Report, and any errors that it may contain, are however all mine.

1.10. The Terms of Reference for the Review were cleared for publication, alongside the Home Office Report, on 9 February 2023. I launched a public consultation on the same day, supplemented a week later by a Specific List of Topics in which I was allowed to give a little more detail (though less than I had wished) on the issues I had been asked to consider.[11] The responses to the consultation were few but of high quality. Some respondents were prepared to have their contributions published; others wished their responses to remain confidential. Responses in the former category are referred to in this Report.

1.11. Meetings with government departments, LE and UKIC were arranged for the Review team by the Investigatory Powers Unit (**IPU**) within the Home Office, to whom I am grateful. In particular, the meetings with all three intelligence services were numerous, thorough and detailed. The team had the use of a secure room in Thames House for the purpose of sensitive discussions and reviewing classified documents. The Review team arranged other meetings, at the request of those

[10] Brief bios are here for Natasha Barnes and John Davies. The TAP, provided for in IPA s246 and set up on the recommendation of the RBPR, advises the IPC on the impact of changing technology and its impact on privacy.

[11] The Terms of Reference and List of Specific Topics are at Annex 2 to this Report.

seeking them or to follow up on written responses to our consultation. A list of those interlocutors who were prepared to be identified is at Annex 3 to this Report.

1.12. Some of the particular topics I was asked to address were described less than fully in my Terms of Reference and List of Specific Topics. It is also the case that the government's position on some issues evolved during the currency of the Review. For these reasons, my own consultation should not be seen as a substitute for public and parliamentary scrutiny of any future legislative proposals, including should it so wish by the ISC, which has access to classified material and statutory responsibility for the oversight of UKIC. I hope that this Report will be a starting point for further exchanges of views, culminating in the parliamentary scrutiny that any Bill will require and that it is not the intention of this Report to pre-empt in any way.

1.13. I have not made formal recommendations on all the topics I was asked to address. Sometimes this was at the request of the Home Office itself, because no policy decision has yet been taken on whether to seek legislative amendment,[12] or because established discussions between regulators, government and others remain to be concluded.[13] In other respects it was because unforeseen complexities emerged during the process of my Review, which required broader consideration than the Review team was able to give them.[14] I have however arrived at a clear position on most of the issues I was asked to address, including the priority issue relating to Bulk Personal Datasets. On the others I have tried to summarise the points that will need to be considered before a concluded position can be reached.

This Report

1.14. This Report was submitted to the Home Office on 17 April 2023, for security checking prior to publication.[15] Some relatively minor changes were called for as a consequence of that process, whose purpose is to ensure that no inadvertent disclosures are made of a kind that could damage national security. No pressure was exerted on me to alter any views expressed in this Report, and any attempt to do so would have been rejected without hesitation.

---

12 DRN Issue 2 (5.29 below); Warrantry Issue 4 (8.29 below).

13 This was the case in relation to an issue concerning error reporting which I was originally asked to consider.

14 Definition Issue 3 (6.23 below); TEW Issue (7.13 below).

15 As required by my Terms of Reference (Annex 2), §5.

1.15. My Terms of Reference gave me the option of producing a classified annex to this report, for the benefit of the Prime Minister and the ISC. However, the purpose of this Report is to inform the parliamentary and public debate on the Bill. Its conclusions faithfully reflect my assessment of all the evidence I have examined. Should the ISC wish to see further detail, it can request briefings, or a sight of the many classified presentations that were made to the Review team. I concluded, as I did when preparing AQOT and RBPR, that little would be gained by producing a secret annex that could not be read by the Report's intended audience.

2. RECENT DEVELOPMENTS

Introduction

2.1. My Terms of Reference invite me to consider the operation of the IPA '*in light of the technological changes and evolving threats which have emerged over the last five years*' and '*by reference to likely future developments in ways of working and technology*'.[16]

2.2. Some of the specific changes that I am asked to consider (in particular those at Chapters 6-9 below) are more of a reaction to practical experience of operating under the IPA than to recent changes to the threat picture or technical capabilities. Others (the proposed changes to BPDs, ICRs and DRNs) are a response both to such practical experience and to specific technical or technological developments that are best explained, to the extent possible in a public document, in the individual chapters devoted to them.

2.3. The evolving threat picture and the technological direction of travel are nonetheless relevant, including to the medium and long-term shape of investigatory powers legislation. This chapter sketches some of the apparent trends, past and future, and their relationship to the IPA.[17]

The threat picture

2.4. The threat picture has developed significantly, and in some respects predictably, since 2018. Terrorism is still widely feared; but while it was relatively recently perceived by the public as a uniquely serious threat,[18] it has been overshadowed in recent years by other factors including health security and hostile state activity.[19]

2.5. Some important developments had not been widely predicted, a point made by the Prime Minister in March 2023:

---

16 Terms of Reference (Annex 2), §5.

17 I am particularly grateful to John Davies for his input on the technical side.

18 The figures are remarkable, in the UK and across the West: see The Fly in the China Shop, my Hague Lecture of October 2017.

19 Strikingly, the Annual Threat Assessment of the US Intelligence Community (February 2023) starts with six chapters on China, Russia, Iran, North Korea, climate change/environmental degradation and health security before turning, in a seventh chapter headed Additional Transnational Issues, to developments in technology, trends in digital authoritarianism and malign influence, nuclear proliferation, global economic consequences of the Russia-Ukraine war, migration, transnational organised crime and, finally, global terrorism.

> '[W]hat could not be fully foreseen in 2021 was the pace of the geopolitical change and the extent of its impact on the UK and our people. We learned from COVID-19 just how much impact events that begin overseas can have on our lives and livelihoods at home. Since then, Russia's illegal invasion of Ukraine, weaponisation of energy and food supplies and irresponsible nuclear rhetoric, combined with China's more aggressive stance in the South China Sea and the Taiwan Strait, are threatening to create a world defined by danger, disorder and division – and an international order more favourable to authoritarianism. Long-standing threats from terrorism and serious and organised crime are enduring and evolving, and may find new opportunities in events like the Taliban takeover of Afghanistan. Other transnational challenges such as large-scale migration, smuggling of people, narcotics and weapons, and illicit finance have become more acute, with grave human costs and strain on our national resources.'[20]

2.6. State threats exist not only at the geopolitical level but in more immediate contexts as well. Physical threats are exemplified by the Salisbury poisoning of 2018 and the assassination programme used by Iran against regime opponents. British and American intelligence chiefs have described covert pressure applied across the globe by the Chinese Communist Party as '*[t]he most game-changing challenge we face*', referencing economic espionage, intelligence-gathering, the buying of influence and cyber-attacks by '*Advanced Persistent Threat*' groups.[21] The Russian '*covert toolkit*', similarly, includes '*cyber attacks, disinformation, espionage, democratic interference, and the use of Putin-aligned oligarchs and others as tools for influence*'.[22]

2.7. Turning from national security to serious organised crime, organised crime groups (**OCGs**) exploit migrants through extortion, kidnapping and human trafficking, including sex trafficking and forced labour or modern slavery. These organisations also continue to pose a direct threat through the production and trafficking of illicit drugs, massive theft, financial crimes and money laundering. There has been a large-scale increase in online child sexual abuse (**CSA**),[23] a rapid increase in the

---

20 *Integrated Review Refresh 2023 – Responding to a more contested and volatile world*, March 2023, Foreword.

21 Joint Address by MI5 and FBI Heads, July 2022. Equally significant is the ability of China to spread its authoritarian values by the export of control and surveillance technologies and by increasing involvement in standards-setting bodies: see *If China is the question, what is the answer?*, the 2022 RUSI Annual Security Lecture delivered by Jeremy Fleming, Director of GCHQ (November 2022), and cf. *Human Intelligence in a Digital Age*, a speech by MI6 Chief Richard Moore (November 2021).

22 Ken McCallum, MI5 annual threat update, November 2022; see also the ISC's Russia Report, published in July 2020 (HC 632).

23 The sheer scale of online sexual abuse, and some of the impediments to detecting its perpetrators, were explained in Part F.3 of the Report of the Independent Inquiry into Child Sexual Abuse (October 2022).

volume of cyber-enabled fraud,[24] and global growth in sophisticated, high-impact ransomware attacks.[25]

2.8. Parliament has recognised the growing threat from hostile state activity in the current National Security Bill, landmark legislation comparable in its scope to the Terrorism Act 2000. The Online Safety Bill also before Parliament is an ambitious attempt to tackle illegal content and activity by regulating internet platforms. But such laws are no substitute for covert investigatory powers, used to detect and counter the threats to UK individuals, interests and values that are variously posed by hostile regimes, organised crime groups and serious criminals. As all these activities shift increasingly online, it is obvious that LE, supported where appropriate by UKIC, must be equipped to follow them.

Technological developments

2.9. Privacy International correctly points out that most of the technological trends observed since 2016 were predicted at the time that the IPA was being planned.[26] But those developments continue apace. Internet services are launched, become wildly popular, and then decline or disappear within a few years. Data is generated in more places, in more formats, and by more different entities than before. Cloud services have increasing capabilities. More data is openly accessible online, and more companies are dedicated to collecting and analysing it for advertising insights.

2.10. Constant changes in the global communications network and the gradual rollout of end-to-end encryption on apps makes bulk and targeted interception more difficult. Partial alternatives such as targeted equipment inference are facing ever increasing on-device security from the main equipment providers. UKIC, therefore, is forced to keep upgrading its capabilities and working harder to keep pace.

2.11. Perhaps the most striking development since 2016, because it is exponential rather than linear in nature, has been the rapidly improving practical applications of artificial intelligence (**AI**) and machine learning (**ML**).[27] ML has now become a

---

24 The Office for National Statistics recorded a 25% increase in fraud between 2019/20 and 2021/22, with the proportion of frauds that are cyber-related increasing from 53% to 61% over the same period. Hacking offences more than doubled.

25 The cybercrime threat to the UK was summarised by the National Cyber-Security Centre (**NCSC**) in its 2022 Annual Review.

26 Response to the consultation §§2.1.3-2.1.5, referencing AQOT Chapter 4.

27 ML is a sub-area of AI, but no widely accepted definition of either term exists. The government's latest policy paper, A pro-innovation approach to AI regulation (March 2023) at §3.2.1 does not attempt a

fast-moving technology area in the commercial and academic worlds, with progress being driven by developments such as deep learning, large language models, improved training methods for models, and the availability of cloud-provided compute and storage at sufficient scales for anyone to get involved. Recent years have been distinguished by the sheer scale of the databases used for training.[28]

2.12. Well-known breakthroughs such as AlphaGo and AlphaFold from DeepMind[29] have driven the expectations and ambitions of investors, who have in turn provided large amounts of money for AI start-ups and patents. There have also been big improvements in large language models (**LLMs**), exposed to the public through chatbots like Open AI's ChatGPT. Language tools such as speech to text and language translation tools appear as standard services within large-scale cloud providers.

2.13. Looking to the future, it may not be fanciful to anticipate the longer-term impact of AI in creating increasingly capable digital entities, superior to humans in capabilities such as knowledge retention, data processing and summarisation. The digital assistant which today plays a song or provides a weather forecast on command may increasingly become what one might call a digital proxy, tasked with replicating human functions, including for example by online interactions with the digital proxies of others. In such a world, we may expect some human decision-making facilities to atrophy, even if '*artificial general intelligence*', in the

---

definition but suggests that AI systems are characterised by their combination of *adaptivity* and *autonomy.* The EU's draft AI Act, which aspires to be as influential internationally as the GDPR, defines AI in Article 3 as software developed with certain techniques and approaches which '*can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*'. Those techniques and approaches are listed in Annex I to the Act under three heads, of which the first is '*machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning'*. Machine learning trains computers on historic data and enables them to modify or adapt their approach without human direction: its various techniques are described with clarity by Peter Wlodarczak in *Machine Learning and its Applications* (CRC Press, 2020).

28 One analysis of ML systems distinguishes the '*pre-Deep Learning Era*' before 2010 from the '*Deep Learning Era*' (c. 2010-2015) and the '*Large-Scale Era*', starting around 2015 with the release of large-scale models such as AlphaGo: Sevilla et al., *Compute Trends Across Three Eras of ML*, 2021. The authors observed that before 2010 training compute (the processing power used to train a model) grew in line with Moore's law, doubling roughly every 20 months; and that since the advent of Deep Learning in the early 2010s, the scaling of training compute has accelerated, doubling approximately every 6 months.

29 DeepMind, founded in London in 2010, was sold to Google in 2014. AlphaGo and its successors have used deep learning techniques to achieve mastery at the game of Go. AlphaFold has revolutionised the science of protein structure prediction, an important goal for drug design and biotechnology.

sense of autonomous systems which surpass human capabilities and continue to develop without human control, remains a distant fantasy.[30]

2.14. Of the developments mentioned in this section some (increasing quantities of data, and improved techniques for analysing it) favour UKIC and LE; others (fragmentation of providers, end-to-end encryption) make their work more difficult. AI will no doubt help to enable both threats to our security and those who seek to mitigate or defeat them: which (if either) will prove more significant cannot at this stage be reliably predicted.[31] I wrote in 2015:

> 'criminals and enforcers are locked in a digital arms race, where neither can be sure of having the upper hand'.[32]

As of today that remains the case, though there can be no guarantee that it will remain so.

2.15. What is hard to envisage, at any rate without genetic engineering or behavioural control on a currently unthinkable scale, is a fundamental change in the '*crooked timber of humanity*'. Warfare, oppression, acquisitive crime and sexual offending are set to persist, whether they are perpetrated offline or online, by humans or by their digital agents. A free and orderly society will depend, in the last resort, on there being effective means of preventing, detecting and constraining such ills without impinging more than is necessary on the exercise of vital human rights and freedoms.

The impact of technological change on UKIC and LE

2.16. The Review team spoke to the capability development and operational teams in UKIC and LE, to improve our understanding of how technology changes have impacted on, or enabled, their delivery of technical systems and insights from data.

2.17. The speed of technology upgrades, the increasing amount and diversity of data and the gradual tightening up of security on the devices and communications services used by potential subjects of interest all impose an increasing load on operational teams, forcing them to be more efficient. Increasingly they have to do

---

30 Not everybody sees it as such: N. Bostrum, *Superintelligence: Paths, Dangers, Strategies* (Oxford, 2014); Ian Hogarth, 'We must slow down the race to God-like AI', Financial Times, 13 April 2023.

31 The transformative potential of AI across every field of human endeavour, and its potential to '*learn, evolve and surprise*' is sketched out for the general reader in Henry Kissinger, Eric Schmidt and Daniel Huttenlocher, *The Age of AI* (John Murray, 2021).

32 AQOT §13.23(a).

more engineering work to support the same number of human analysts and investigators.

2.18. The technology response of UKIC and LE is to avoid duplication of effort, use more automation tools so as better to select and prepare data for human decision-makers, and work together more with partners. AI and ML offer an opportunity to keep up with this load, and even make operational progress, if they can be used with suitable necessity and proportionality constraints, and if authorisation and oversight functions can (including by their own use of AI) keep up with the innovators.

2.19. Data is still often held in large secure buildings, but increasingly on utility computing platforms where it can be shared with universities or start-ups, or accessed by an officer in a war zone or seconded to a partner. The world of UKIC is becoming a mixture of shared systems and services, with specialised tools built on top of them. The data itself is in a wide diversity of forms: not just phone calls, messages, and emails. The important information might (hypothetically) be in a social media bio, or written on a whiteboard in the background of a secure video call, or from a human source commenting on how many likes a post received on a suspect's feed within a secure online forum.

2.20. UKIC is leveraging partnerships to the greatest extent possible to accelerate development and deployment of needed capabilities. Specialised entities such as NCA, CTP and HMRC form a bridge between UKIC and general policing, with the most intrusive capabilities restricted as the IPA demands to the most serious crime investigations. General policing is assisted by analysis of communications data (**CD**) and the less intrusive aspects of targeted equipment interference (**EI**).

2.21. There will always be different opinions about how widely available certain capabilities should be, driven by the different roles of the parties and by the sensitivities and fragility of some of the more powerful capabilities. There will be future tensions in this area around use of, for example, commercial hacking tools, where the larger police constabularies may want to start using capabilities historically exploited only by specialised LE entities or UKIC.

2.22. Automation in these areas requires efficient management of large-scale computing resources to rapidly process large amounts of data, effectively manage storage, and deal with the complexity of varied data sources. UKIC has been doing this for many years. The use of commercially available solutions can however address many of its requirements (e.g. rich compute, storage and data

management services), allowing UKIC to focus more on mission-specific tasks that cannot be achieved with commercial tools.

2.23. AI-driven automation possibilities around speech, text and image processing will grow quickly, and become part of the standard toolkit of every business, and every UKIC or LE agency. The AI tools will climb the value stack, replacing human effort in an increasing range of tasks.

2.24. AI underlies existing capabilities such as the Child Abuse Image Database (**CAID**), which identifies victims and perpetrators of CSA,[33] and cyber-defence against malicious actors.[34] Other automated techniques, such as live facial recognition surveillance by police, have been more controversial.[35] ML automation techniques (e.g. image to text conversion, language translation, audio processing, classifiers to pick information of interest out of huge datasets) have been used by UKIC for many years. To date, ML tools have been used to triage large volumes of data in order to support onward human decision-making, with the proportion of data subject to automated enrichment increasing through time.

2.25. UKIC and LE can use externally-produced tools to automate their work, but it is essential that they adhere to strong ethical and oversight frameworks when they use AI techniques as part of their use of investigatory powers. The ethics of AI is one of the most pressing of contemporary issues, extending far beyond the world of intelligence and policing. The many dilemmas that it throws up are not capable of being resolved by UKIC on its own, and will pose huge challenges to the existing oversight mechanisms which it is proposed should bear the load.[36] Nonetheless, I

---

33 The government announced in 2019 that the CAID was being upgraded by the addition of a fast-forensic tool to rapidly analyse seized devices and find images already known to law enforcement; an image categorisation algorithm to assist officers to identify and categorise the severity of illegal imagery; and a capability to detect images with matching scenes to help identify children in indecent images in order to safeguard victims.

34 National Cyber Security Centre (NCSC), *Intelligent Security Tools: assessing intelligent tools for cyber security* (2019).

35 Metropolitan Police, *Facial Recognition Technology*. Use of the technology by South Wales Police was declared incompatible with human rights, data protection and equality law in *R (Bridges) v CC South Wales Police* [2020] EWCA Civ 1058; see also E. Radiya-Dixit, *A Socio-Technical Audit: Assessing Police Use of Automatic Facial Recognition*, Minderoo Centre for Technology and Democracy, Cambridge University, October 2022.

36 The government published in March 2023 its policy paper A pro-innovation approach to AI regulation, underpinned by five principles described as safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress. As the title suggests, the framework was designed to be flexible, with its application devolved to sectoral regulators. It contrasts with the approach of the EU's draft AI Act, which will ban applications and systems deemed to create an unacceptable risk and subject some others to specific legal requirements. The call by a UK parliamentary committee for a single national body to govern the use of new technologies in law enforcement has been rejected: House of Lords Justice and Home Affairs Select Committee, *Technology*

have been impressed by the work that has been done within UKIC on the ethics of AI,[37] and hope that in some form at least it will be possible to make more of it public as a means of reassurance that ethical and oversight issues are being addressed on the principled basis that is required.

2.26. Sharing sensitive capabilities with others is always difficult. It requires trust, and needs each party to believe that others in the group are contributing sufficiently to outweigh the additional risk of them being involved.

2.27. Using AI/ML for intelligence purposes will also demand cooperation. The partnerships will be both the traditional ones, but also newer groups, including academia and industry partners, large and small. UKIC wants to be a valuable partner in these innovation groups to gain early advantage of new inventions. The prize will be to allow nimble and effective cooperation to proceed without prejudicing the ethical and oversight frameworks on which the democratic legitimacy of UKIC depends.

The consequences of technological change for the IPA

2.28. The IPA marked a decisive change in the UK's legislative regime governing investigatory powers, particularly in terms of transparency and oversight. These improvements have undoubtedly been helpful in securing parliamentary and public support for the extensive powers that the Act confers and judicial approval in the UK and elsewhere, as well in securing the mutual recognition on which the ground-breaking UK-US Data Access Agreement (**DAA**) is based.[38]

2.29. In terms however of the technical concepts on which it was built, the IPA was in many respects more of an upgrade to RIPA, itself conceived at the end of the last century.

2.30. Though attempts were made to maximise the life of the IPA by drafting it so far as possible in a technology-neutral manner, some of its language (and indeed the

rules? The advent of new technologies in the justice system, March 2022; government response, July 2022.

[37] GCHQ published *Pioneering a New National Security: the Ethics of Artificial Intelligence* in February 2021, in which it said that it was developing an AI Ethical Code of Practice. GCHQ's open-source release of the machine-learning tool Bailo is another example of public commitment to AI ethics. See, most recently, the CETaS report *Privacy Intrusion and National Security in the Age of AI*, May 2023.

[38] The principle of judicial approval of warrants is of particular significance in the US (and Canada), where this is the norm: see AQOT §§11.15-11.28. It is also viewed by the ECtHR as the premium level of oversight.

language of comparable laws across the world) already recalls a time when systems were simpler in architecture, and less fluid and connected. For example:

- The concept of a ***telecommunications operator***, once restricted to providers of telephony services, is now used to embrace bodies as various as vehicle manufacturers and hotel chains.[39]

- The category of ***communications data***, once explicable as akin to '*the writing on the envelope*' of a communication between humans, now embraces location data generated automatically by a mobile phone when its owner is asleep – something closer to the product of intrusive or directed surveillance, which fall (perhaps incongruously) outside the IPA regime.[40]

- The techniques of ***interception*** and ***EI*** are increasingly convergent and often encompassed by combined warrants,[41] calling into question the appropriateness of their terminology and, more substantively, the different treatment in law of these two capabilities and their respective products.[42]

2.31. More generally:

- Rules based on the ***location*** of a given function, or of given data, must face the challenge of an online world in which functions are devolved and geographical barriers count for little.[43]

- The IPA's focus on how bulk data may be acquired or retained may need to evolve towards a focus on how ***bulk data is used*** – not simply by

---

39 The extent to which such bodies may be acting as TOs was often described to us as obscure and confusing. See Home Office Report at p11 and Definition Issue 1 in Chapter 6, below.

40 The reason is historical: location data has always been generated when a call is made from a mobile phone (or indeed from a landline). Some of the issues relating to the definition of CD are addressed under Definition Issue 1 at 6.7-6.14 below.

41 See IPCO's 2021 annual report, §8.16, disclosing that IPCO now conducts combined inspections of these capabilities at MI5.

42 In particular the prohibition on the evidential use in criminal proceedings of intercept (but not the product of EI) in IPA s56, a topic which falls outside the scope of my Terms of Reference but on which I heard strong views from different perspectives. On the borderline between interception and EI, see *SF and others v NCA* [2023] UKIPTrib3. The complexity (and some might think artificiality) inherent in having to decide whether data is in the course of transmission or at rest when it is intercepted is evident from the judgment of the Court of Appeal in *A and ors.v R* [2021] EWCA Crim 128: see the Home Office Report at pp 17-19. See further, on the definition of interception, Definition Issue 3 (6.21-6.23 below).

43 Data may for example be in a replicated store across two cloud providers, who move virtual machines between data centres to maintain resilience. Processing may be a joint endeavour, starting on a UK HQ system, calling out to a partner's analytic function and feeding in further data from a commercial data broker's store.

improved oversight of selectors[44] but by increasingly sophisticated bulk analytics and AI techniques that are applied to personal data.

- In the context of ML models in particular, the IPA's focus on the right to privacy may need to be broadened to reflect more fully the other data rights that can be impacted by biased or poorly-trained models, including ***transparency, algorithmic fairness and non-discrimination***.

- This in turn has implications for ***oversight***: it is for consideration whether the Information Commissioner's Office (**ICO**) with its special expertise in data processing and AI should have an enhanced role in intelligence oversight, alongside IPCO.[45]

2.32. These are among the points that will need to be considered the next time that change to the IPA is contemplated: see Chapter 10, below.

[44] As required by the ECtHR in its *Big Brother Watch* judgments: see Annex 4 at §2. Graham Smith in his response to the Review (§21) described a focus on selectors and search criteria as '*faintly old-fashioned*', given the application to intercepted material (particularly CD), as disclosed in RBPR, of '*more sophisticated analytical techniques such as anomaly detection and pattern analysis*'. His full response can be found at https://drive.google.com/file/d/1AuBhW8tzAw5yrZIpZVrtZoqQUVS6aWyK/view

[45] ICO already has oversight of the scheme under which the NCA mirrors the operation of IPA Part 7: 3.19 below.

3. BULK PERSONAL DATASETS

Utility of BPDs

3.1. Anyone who has made use of Wikipedia, or who manages a membership list for a club or forum, is familiar with the idea of a personal dataset. Outside the intelligence context, the uses of large-scale personal datasets are myriad:

- The ***Police National Computer***, to be replaced by the Law Enforcement Data Service, provides access to a centralised source of information concerning individuals, property and vehicles.
- ***Financial and commercial records*** can help business organisations detect fraud, decide whether an individual is creditworthy and determine how advertisements can be most effectively targeted.
- ***NHS data*** drove the response to Covid-19, and facilitates the development of new medical technologies.
- In recent years vast sets of personal data, including ***facial images and speech samples***, have been used to train the ML models that are set to transform multiple aspects of human and commercial life.

3.2. The collection and analysis of intelligence by UKIC has relied for more than a century on BPDs[46] on their own, in combination and in conjunction with other sources of intelligence.[47] Remarkably, however, the '*capability*' was not avowed until the ISC revealed it in March 2015.[48] Both the size and the number of BPDs of interest to UKIC have increased massively since the advent of the internet, with the explosion of personal data stored on searchable electronic databases.

---

[46] A BPD is defined in the IPA as '*a set of information that includes personal data relating to a number of individuals … such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions*': IPA s199(1)(a)(b). A BPD is '*retained*' by an Agency if after initial examination of its contents it is held, or to be held, electronically for analysis in the exercise of those functions: s199(1)(c)(d).

[47] The submission to the Review from Tony Comer OBE, former departmental historian of GCHQ (Annex 5 to this Report), explains for example that during the First World War the War Trade Intelligence Department kept an index card database of ships, seamen and traders to develop a mainly complete picture of transatlantic shipping, and refers to the diplomatic '*personality indexes*' that were compiled in the inter-war period from both intercept and open-source material. See further RBPR §2.69, referring to an MI5 witness statement before the IPT.

[48] ISC, *Privacy and Security: a modern and transparent legal framework*, HC 1075, March 2015, §158. BPDs fell outside the Terms of Reference for AQOT: they were accordingly referred to only in passing (at 7.69-7.70).

3.3. The categories of BPDs retained by UKIC were summarised in 2015 in the following terms:

- Law enforcement/intelligence: datasets containing operationally focused information from law enforcement or other intelligence agencies;
- Travel: datasets containing information which enables the identification of individuals' travel activity;
- Communications: datasets allowing the identification of individuals where the basis of information held is primarily related to communications data, e.g. a telephone directory;
- Finance: datasets allowing the identification of finance-related activity of individuals;
- Population: datasets providing population data or other information which could be used to help identify individuals, e.g. passport details; and
- Commercial: datasets providing details of corporations/individuals involved in commercial activities.[49]

3.4. UKIC acquires BPDs through both overt and covert channels. While the complete list of BPDs held by UKIC was described in 2016 by the then Chair of the ISC as '*pretty mundane*',[50] some of the datasets are extremely large and their number and variety is increasing rapidly. I noted in the RBPR that BPDs generally contained basic biographical details on individuals that correspond to the definition of '*identifying data*', but that a small proportion contained material that is comparable to the content of communications as defined in the IP Bill. It was confirmed to me that this remains the case.

3.5. The value of BPDs to UKIC was beyond question, even seven years ago. MI5, MI6 and GCHQ each provided statements of utility to my 2016 Bulk Powers Review,[51] which were confirmed by the internal documentation inspected by the Review. I concluded:

> 'I have no hesitation that BPDs are of great utility to the SIAs. The case studies that I examined provided unequivocal evidence of their value. Their principal utility lies in

49 RBPR §2.71, citing evidence given by MI5 to the IPT.

50 Dominic Grieve QC MP: Hansard HC 7 June 2016, vol 611 col 1064, quoted in RBPR §2.71.

51 RBPR Annexes 5-7, summarised at §§8.3-8.5. The NCA also characterised bulk data as offering '*a different and unique intelligence picture, not obtainable through other means*': *ibid.*, 8.6.

the identification and development of targets, although the use of BPDs may also enable swift action to be taken to counter a threat.

BPDs are already used elsewhere, in the private as well as the public sector, with increasing sophistication. … As I concluded in AQOT 8.106: "*It may legitimately be asked, if activity of a particular kind is widespread in the private sector, why it should not also be permitted (subject to proper supervision) to public authorities.*"

BPDs are used by the SIAs for many purposes: for example, to identify potential terrorists and potential agents, to prevent imminent travel, and to enable the SIAs to prioritise work. It will often be possible, in a given instance, to identify an alternative technique that could have been used. However many such alternatives would be slower, less comprehensive or more intrusive. The value of accurate information, obtained at speed, is considerable. I accept the claims of MI5 and MI6 that their work would be substantially less efficient without the use of BPDs and GCHQ's claim that it finds BPDs useful to enrich information obtained through other means.

In some areas, particularly pattern analysis and anomaly detection, no practical alternative to the use of BPDs exists. These areas of work are vital, since they can provide information about a threat in the absence of any other intelligence seed. …

The use to which bulk data can be put is in the course of rapid evolution. MI5 recognised in July 2015 that the development of new technologies and data types, including ML and predictive analytics, offered "*additional promise*" in this field. Future decision-makers authorising and approving the use of BPDs will have to be aware of these technological advances, and the effect that they have both on the availability of alternatives and on the extent of intrusion involved in the use of BPDs.'

3.6. Fifteen redacted case studies, their full details verified by the Bulk Powers Review team, illustrated the value of BPDs in agent recruitment, target discovery, target development, anomaly detection, pattern analysis and disruptive action.[52] The majority of those studies related to counter-terrorism, which comprised the great majority of UKIC's work at the time. Others concerned counter-espionage and counter-proliferation. GCHQ and MI5 have recently prepared for publication some further case studies on the use of BPDs, which are at Annex 6 to this Report.

3.7. The RBPR described the use made of BPDs by UKIC in the following terms:

'The SIAs do not claim to employ searching techniques any more advanced than those available commercially; indeed I was told that they see themselves as "*catching up with the commercial sector*". The examples that we were shown appear relatively straightforward, and were not indicative of the use of BPDs to predict in the highly sophisticated manner attributed to some private sector operatives. But any critical evaluation of the power needs to assume that SIAs have, or will acquire, the capability to make such use of BPDs as the most advanced current and future techniques allow.'[53]

52 RBPR Annex 11; see also the government's Operational Case for Bulk Powers, March 2016.

53 RBPR §2.80.

In similar terms, the Operational Case published by the government in March 2016 had stated:

> 'The security and intelligence agencies hold the data electronically and analysts will only look at the data relating to the minority who are of intelligence interest. The security and intelligence agencies do this by asking specific questions of the data to retrieve information of intelligence value.'[54]

3.8. The uses of BPDs are evolving rapidly. It has been said that big data analytics can support national security decision-making in a number of (overlapping) ways: ***anomaly detection*** (which identifies items, events or observations that do not conform to an expected behaviour or pattern); ***association mining algorithms*** (which discover relationships and patterns hidden in large datasets); ***classification algorithms*** (which assign objects in a collection of data to target categories or classes); ***clustering*** (grouping objects or data points together based on notions of similarity); ***link analysis*** (used to identify nodes and networks connecting people, organisations and other entities); and ***ML*** (algorithms that can independently adapt and learn from the data they process, and synthesise human-readable summaries and data views).[55]

3.9. Bulk collection and bulk analysis techniques are used by UKIC to discover and confirm new investigative '*seeds*'. Seeds from UKIC's own work or from partners can then be developed into usable intelligence using BPDs and transformation tools including machine learning models. When UKIC works to support LE, it provides strongly-supported intelligence leads, which are then investigated by LE with a view to obtaining court-quality evidence. Thus, when a person is charged with accessing child sexual abuse imagery, it will not be because a behavioural algorithm suggests that they may be guilty but because prosecutors consider that there is a reasonable prospect of conviction on the basis of evidence that can be presented to a court.

3.10. Significant increases in the type and volume of data created externally means that ML techniques are proving useful to UKIC in supporting the coverage of subjects of interest. For example:

---

54 Operational Case for Bulk Powers, March 2016, 10.1.

55 D. Van Puyvelde, S. Coulthart, M. Shahriar Hussain, *Beyond the buzzword: big data and national security decision-making*, International Affairs, Volume 93, Issue 6, November 2017, pp 1397–1416, summarised by its authors in *National security relies more and more on big data. Here's why*, Washington Post, 27 September 2017. See, further, the CETaS research report by Alexander Harris, Eleanor S., Emma Bradford and Ardi Janjeva, *Behavioural Analytics and National Security*, March 2023, which emphasises text analysis, social network analysis and geospatial analysis as areas of significant potential for the scaled application of behavioural analytics (Chapter 2) and contains three fictitious cases that are said to demonstrate the potential utility of behavioural analytics in the near future (Chapter 5).

- BPDs have been used by GCHQ's AI researchers to build a semantic language search model. This machine learning model has then been applied to search other warranted data for key words in both English and a foreign language simultaneously, thus enabling the triaging of documents to be carried out regardless of the analyst's knowledge of the foreign language. This significantly speeds up the process of identifying relevant intelligence in foreign languages, enabling more analysts to work at the pace of the threats that are faced.

- MI5 told us that datasets accessed via the IPA can support the development of detectors for imagery of national security concern such as weapons. Analysts label the content to allow ML models to be trained to detect firearms in images. These models can then help focus the future work of those analysts, who can spend more time on the most promising images.

- Techniques of significant potential value include optical character recognition, machine translation, speech-to-text and speaker identification.

3.11. The training of ML models requires large quantities of data that is representative of the type of data on which the model will be deployed, but which is voluminous enough to overcome or minimise any inherent biases. Sometimes personal data is required, though personal data can also feature in ML training datasets even when it is not the primary interest.[56] The best data on which to train models tends to be open source, publicly available and sometimes commercially curated. When building models, intelligence services are not interrogating the data to identify individual records of intelligence interest, but are using the structure and attributes of the whole dataset to build capability and tools to help deliver their intelligence functions. This activity is likely to continue, and to grow, in the future.

Regulation of BPDs

3.12. When it avowed the use of BPDs by UKIC,[57] the ISC summarised the internal controls operated by each intelligence service on the acquisition and use of BPDs. It criticised the absence of '*restrictions on the acquisition, storage, retention, sharing and destruction*' of BPDs, and recommended that judicial oversight (which

[56] For example, sets of weaponry images may not sound like personal data: but they will nonetheless constitute BPD when identifiable features such as faces are captured in the broader image.

[57] *Privacy and Security: a modern and transparent legal framework* HC 1075, March 2015, §158..

was already practised on a retrospective, six-monthly basis by the Intelligence Services Commissioner) be placed on a statutory basis.

3.13. The ISC's recommendations were accepted by the government, which in a reference to what was to become IPA Part 7 stated:

> 'Part 7 of the draft Bill provides explicit statutory safeguards governing the Agencies' acquisition and use of Bulk Personal Datasets. These include a warrantry regime with an authorisation process that is consistent with other bulk capabilities in the draft Bill.'[58]

3.14. The BPD regime in IPA Part 7 entered into force for most purposes in the summer of 2018. It did not in fact govern the *acquisition* of BPDs, but rather provided what were described as '*robust new safeguards that apply to the retention and examination of bulk personal datasets*'.[59] These safeguards, as flagged in the government's response to the ISC, resemble in most respects those applied by Part 6 to the other bulk powers governed by the IPA.[60] This is despite the fact that the use of BPDs, unlike the Part 6 capabilities, is widespread and not reserved to UKIC. Prominent among the safeguards is the '*double lock*' requirement that warrants be both authorised by the Secretary of State[61] and approved by a Judicial Commissioner.

3.15. The Part 7 regime was summarised, as clearly as its complexities permit, by the Divisional Court in a judgment of 2019:

> '211. Section 200 generally prohibits an intelligence service from retaining a BPD or examining a BPD it has retained without obtaining a warrant for that purpose, either a "class BPD warrant" or a "specific BPD warrant". Thus, the 2016 Act introduces a new and additional warrant requirement for BPD. Section 201 disapplies that requirement where the intelligence service obtained the BPD under a warrant or other authorisation given under the 2016 Act, or the BPD is being retained or examined for the purpose of enabling any information it contains to be destroyed ...
>
> 212. Under section 199(1) of the 2016 Act, an intelligence service retains a BPD where: (a) it obtains a set of information that includes "personal data" relating to a number of individuals; (b) the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of intelligence interest; (c) after any "initial examination" of the contents, the intelligence service retains the set of information for the purpose of exercising its functions; and (d) the set is held, or is to be held, electronically for analysis in the exercise of those functions ...

---

58 Government Response to the ISC Report on Privacy and Security, December 2015, p. 15.

59 Government Factsheet accompanying the IP Bill, 2016.

60 Bulk interception (Part 6 chapter 1), bulk acquisition of CD (Part 6 chapter 2) and bulk EI (Part 6 chapter 3). The operational case for each of these powers was examined in RBPR.

61 'Secretary of State' means any one of Her Majesty's Principal Secretaries of State: Interpretation Act 1978, Schedule 1.

213. “Personal data” means (a) data within the meaning of section 3(2) of the Data Protection Act 2018 (i.e. relating to an identified or identifiable living individual) which is subject to processing described in section 82(1) of that Act (processing by an intelligence service of personal data wholly or partly by automated means, etc), or (b) data relating to a deceased individual which would fall within (a) if it related to a living individual. Section 220 stipulates time limits for the initial examination of a set of information to determine whether it constitutes a BPD within the meaning of section 199 and, if so, to seek a class or specific BPD warrant. Broadly speaking, the head of an intelligence service has three months to do so where the set of information was created in the UK, and six months where it was created outside the UK.

214. It is common ground that Part 7 does not itself contain any power to obtain a BPD. Rather, the requirement for a BPD warrant concerns the retention and any subsequent examination of a BPD previously obtained under other powers. They may include a warrant issued under section 5 of the Intelligence Services Act 1994 (“ISA”), or exercise of the intelligence services’ “information gateway” powers under the ISA and the Security Service Act 1989, and other powers under the 2016 Act (except for Part 6, Chapter 2).

215. The decision to issue either a class BPD warrant or a specific BPD warrant must be taken by the Secretary of State personally (section 211) and is subject to prior approval by a JC, except where the Secretary of State considers there is an “urgent need” for a specific BPD warrant to be issued (sections 204(3)(e), 205(b)(e) and 208). Where a specific BPD warrant is issued without prior JC approval because of urgent need, the Secretary of State must inform a JC that the warrant has been issued and, within three working days, the JC must decide whether or not to approve that decision. In the event of a refusal to approve the warrant, it ceases to have effect (section 209). The JC may direct the destruction of data retained under the warrant or impose conditions as to the use or retention of such data (section 210).

216. A class BPD warrant authorises the retention or examination of any BPD falling within a class described in the warrant; whereas a specific BPD warrant authorises the retention or examination of any BPD described in that document. Neither type of BPD warrant may be issued (or approved) unless both the Secretary of State and the JC consider that it is necessary on the grounds of national security, for the prevention or detection of serious crime, or in the interests of the economic well-being of the UK in so far as those interests are also relevant to national security. They must also be satisfied that the operational purposes specified in the application for the warrant are purposes for which examination of the BPD described is or may be necessary, and that such examination is necessary on any of the grounds upon which the warrant is considered necessary. In addition, both the Secretary of State and the JC must be satisfied that the conduct authorised by a warrant would be proportionate to what is sought to be achieved (see sections 204(3), 205(6) and 208(1) and (2)).

217. Furthermore, the general duties in relation to privacy in section 2 are engaged. Thus, the Secretary of State and the JC must consider whether what is sought to be achieved by the warrant could be achieved by other less intrusive means. They must also consider any aspect of the public interest in the protection of privacy (section 2(2)) and any consideration relevant to proportionality (section 2(3) and (4)). The JC must consider these matters with a sufficient degree of care as to ensure that he or she complies with the duties under section 2 (section 208(2)(b)).

218. Thus, the issuing of BPD warrants under Part 7 is subject to many of the fundamental safeguards in Part 6 to which we have already referred, including, in particular, the "double-lock" provisions.

219. Furthermore, a BPD may not be retained, or retained and examined, pursuant to a class BPD warrant if the head of the intelligence service considers that the BPD consists of or includes, "protected data" or "health records" (section 206) or that a substantial proportion of the BPD consists of "sensitive personal data". Essentially, "protected data" means (section 203) "private information" (which "includes information relating to a person's private or family life" and all other data in a BPD other than "systems data" or "identifying data" which is capable of being separated logically from that BPD without revealing the meaning of any of the data). An application to retain, or to retain and examine, data within these categories would have to be made as an application for a specific BPD warrant. Additional safeguards in relation to specific warrants covering "health records" and "protected data" are provided by sections 206 and 207…

220. In relation to bulk warrants issued under Chapters 1, 2 or 3 of Part 6, the Secretary of State must consider that satisfactory arrangements are in force for securing safeguards relating to access to, copying, examination and destruction of material (sections 138(1)(e), 158(1)(d) and 178(1)(e); ... These safeguards are more specifically defined in sections 150-1, 171 and 191-2. By contrast, for BPD warrants issued under Part 7, the Secretary of State need only consider that the arrangements made by the intelligence service for storing the BPD or BPDs to which the application relates and for protecting them from unauthorised disclosure are satisfactory (sections 204(3)(d) and 205(6)) and the statute does not go on to lay down any more specific requirements. Nevertheless, there are specific additional safeguards for the examination of BPD or data subject to legal privilege (sections 221-223; …).

221. Sections 213-219 deal with the duration, renewal, modification and cancellation of BPD warrants ... Save for section 219, which we consider below, these provisions largely mirror those applicable to bulk warrants under Part 6.'[62]

3.16. The 24 pages of IPA Part 7 are supplemented by a 74-page Code of Practice, which provides detailed guidance on the procedures that must be followed before BPDs can be retained and examined by UKIC.[63] That Code of Practice is, itself, supplemented by internal procedures within each Agency.

3.17. Standing back from the content of the existing regulatory regime, it is important to recognise its ***relatively narrow scope***. Three general remarks are in order.

---

62 *R (Liberty) v SSHD* [2019] EWHC 2057 (Admin); [2020] 1 WLR 243, §§211-221 (Holgate LJ and Singh J).The Court rejected a challenge to the compatibility of Part 7 with the ECHR (see Annex 4 to this Report at §4, second bullet). That judgment is currently under appeal, but the accuracy of this summary is not in dispute. A more detailed '*overview*' of the Part 7 provisions forms an annex to the judgment.

63 Intelligence services' retention and use of bulk personal datasets Code of Practice, March 2018.

3.18. First, the Part 7 regime applies not to the ***acquisition*** of BPDs but only to their ***retention and examination***. It does nothing to limit the ability of UKIC, or anyone else, to acquire BPDs by whatever means they lawfully can.[64]

3.19. Secondly, the Part 7 regime ***does not apply to LE*** which like UKIC must comply with data protection law but which is subject to no additional statutory requirements relating to retention or examination[65] (though the NCA chooses to mirror the operation of Part 7 by a non-statutory scheme, overseen by the ICO;[66] and Counter-Terrorism Policing expressed a wish to see '*a resilient, dedicated LE legal mechanism to justify the retention and examination of a set of data as a whole'*). Neither does Part 7 or any equivalent apply to the ***public sector, business or third sector***.[67]

3.20. Thirdly, the Part 7 regime does not apply to ***personal data held by third parties*** to which UKIC has access. IPCO conducted an '*extensive review*' of such datasets in 2019 and recommended that the government consider bringing them within IPCO's oversight.[68]

3.21. In short:

- Part 7 applies a rigorous and ECHR-compliant[69] regulatory regime to the retention and examination of BPDs by UKIC.
- That regime is modelled on those devised for the exercise of highly intrusive powers such as bulk interception, which unlike BPDs are restricted to UKIC.
- While sensitive categories of data are subject to additional protection, the principal features of Part 7 – including the double lock, with its complex associated procedures – apply to all BPDs, even those which are already in the public domain and accessible to all.

---

64 These means include, in the case of the SIAs, their powers under the Security Service Act 1989 s2(2)(a) (MI5) and the Intelligence Services Act 1994 ss2(2)(a) and 4(2)(a) (MI6 and GCHQ), known as the information gateway provisions. NB also the Counter-Terrorism Act 2008 s18, which removes restrictions on disclosure from the supplier of information.

65 Part 3 of the Data Protection Act 2018 (**DPA**) governs processing by police and other bodies with investigative functions. Part 4 of the Act, on which the ICO has issued an informative Guide, governs processing by UKIC.

66 The NCA has published its Operating Procedure for BPDs.

67 A table comparing the different legal frameworks that apply to different users of open-source BPDs, prepared at my request by the Home Office, is at Annex 7 to this Report.

68 2019 Annual Report of the Investigatory Powers Commissioner, December 2020, 2.28-2.29.

69 Subject to the outcome of the appeal in the *Liberty* case: Annex 4 to this Report at §4, second bullet.

- No equivalent regime applies to other public and private sector users of BPD, or even to UKIC when it accesses BPDs held by others.

3.22. These unusual and in some respects anomalous features of the Part 7 regime prompt reflection as to whether, as a matter of policy, its scope is correctly defined, bearing in mind that the use of BPDs is normally considered less intrusive than (for example) the use of bulk powers to intercept communications or the hacking of personal devices under the equipment interference provisions.

3.23. The principle of a specific regime applied to UKIC (and not, for example, to LE) can arguably be defended on the basis of UKIC's unique capabilities, including its power to acquire BPDs by means that would be unlawful for others and its ability to combine intelligence gleaned from BPDs with the product of other, highly intrusive, bulk techniques. But to apply the Part 7 regime to BPDs that are used without restriction by public and private bodies at home and abroad is seen by the intelligence services as a problematic constraint on the agility which is essential to their work.

Consultation

3.24. The Home Office Report raised the issue of whether the safeguards in Part 7 are excessive:

> 'The exceptional growth in volume and types of data across all sectors of society globally since the Act has entered into force has impacted UKIC's ability to work and collaborate at the necessary operational pace. The BPD safeguards in the current statutory framework are disproportionate for some types of data, creating a negative impact on operational agility, while also harming capability development.
>
> The safeguards in Part 7 do not account for the way that data and its availability have evolved since the Act passed. In particular, it did not foresee:
>
> - The exponential increase in the use of, complexity, and changing nature of data;
> - The extent to which clouds and commercially available tools would make powerful analysis of datasets possible;
> - The possibility that most data referencing human activity can in theory be resolved to real world identities, rendering datasets that would not previously have been considered BPD within the scope of Part 7 of the Act.
>
> Reform to Part 7 would assist UKIC with the aim set out in the IR to "*take a more robust approach in response to the deteriorating global security environment,*

adapting to systemic competition and a wider range of state and non-state threats enabled by technology".'[70]

3.25. My Terms of Reference asked me to consider the effectiveness of the BPD regime, and whether Part 7 remains fit for purpose. The List of Specific Topics amplified that question by reference to the three issues specifically raised in the Home Office Report: whether the current warrantry process in Part 7 is fit for purpose for all types of datasets, whether the current duration of warrants should be amended, and whether certain powers vested in Agency Heads[71] should be delegated to a Crown Servant.

3.26. Liberty and Privacy International emphasised that they considered the current BPD safeguards to be *'minimal'* and '*wholly inadequate to provide even a basic protection of rights'*.[72] Both strongly resisted any proposal to weaken the existing safeguards. Privacy International considered that there had been no technological changes since 2016 that prevented the objectives of Part 7 from being met.[73] It concluded that there was *'a need for more robust safeguards, not less'*.[74] Liberty also recorded its objection in principle to the bulk powers set out in the IPA.[75]

Operation of the Part 7 regime

3.27. The first step for the Review team was to assess how the Part 7 regime works in practice. With that in mind we spent prolonged periods at each of the three intelligence services, probing the processes that lead to the authorisation and approval of BPD warrants.

3.28. The experience was not an inspiring one. A BPD regime which reads logically enough on the pages of the IPA and Code of Practice is proving cumbersome in practice, particularly at MI5. While adding a dataset to a class warrant can be quite speedily done, the median time required by MI5 in 2018-2023 to add a new class or specific warrant, from identification to judicial approval, was over three

70 Home Office Report, pp. 14-15.
71 IPA ss202, 206, 210, 219, 220 and 225.
72 Liberty response, §8; their full response can be found at https://www.libertyhumanrights.org.uk/issue/liberty-responds-to-home-secretarys-review-of-snoopers-charter/.
Privacy International response, §2.2.3.
73 Privacy International response, §2.1.2.
74 Ibid, §2.3.1.
75 Liberty response, §6.

months. The pressure on time can only increase, in line with pressure to add more warrants.[76]

3.29. All three intelligence services are currently reviewing their authorisation processes to seek and drive out inefficiencies. This exercise is strongly to be encouraged.

- The Review team closely questioned those conducting this exercise at MI5, where it is hoped that administrative simplifications will halve the time taken. Similar reductions are expected across UKIC.

- MI6 is using automated tools to help officers identify protected data, simplifying paperwork and grouping datasets with the same operational purpose, and in respect of which a similar necessity and proportionality analysis applies, on the same authorisation form.

- GCHQ told the Review team that it has devoted significant resource to improving the efficiency of its authorisation processes, led by an individual with considerable experience in this area.

3.30. It has become apparent, however, that the basic structure applicable to BPD cannot be further reformed without amendment to the IPA.[77] While there is acceptance in UKIC and across government that the rigours of Part 7 are appropriate to the most sensitive and intrusive datasets, they are perceived as disproportionately burdensome in their application to publicly-available datasets, specifically those containing data in respect of which the subject has little or no reasonable expectation of privacy. This is not simply (or even principally) because of the authorisation process itself but because of the time-consuming upstream (e.g. identifying sensitive data) and downstream (e.g. handling, examination) requirements.[78]

3.31. We were told that this is causing the intelligence services ***damage to operational agility*** in a number of respects. We were able in many cases to verify this by reference to real-world examples that were presented to us in person by operational teams, most strikingly in MI6.

---

[76] IPCO reported that in 2021, 111 class BPD warrants and 66 specific BPD warrants were authorised and approved: see 2021 Annual Report, March 2023, Table 19.2 and Figure 19.12. I was told that the number of warrants added has increased markedly since then.

[77] Limited results might be achieved by amending only the BPD Code of Practice: but for the most part its requirements are inherent in the Act.

[78] See further 3.38-3.46 below.

3.32. In some cases, the problem was simply one of ***delay***. BPDs can be of rapidly diminishing value, for example in a fast-moving investigation or battlefield scenario. A lengthy authorisation process, even if pursued with all possible speed, occupies the time of data scientists (who are a valuable resource) and may mean that an operational window has closed before the BPD can be deployed. Time spent securing the authorisation of datasets for training ML models can remove the comparative advantage of the resultant models, and/or encourage them to be trained with sub-optimal quantities of data.

3.33. An additional, serious problem relates to ***cooperation with partners***. By way of illustration:

- UKIC teams co-locate with Ministry of Defence (**MOD**) personnel overseas, often in hostile environments. If MOD has acquired a dataset through its own permissions, it is unable to transfer that BPD to the UKIC terminal in the same room as it would need to be warranted. Neither may UKIC officers ask MOD to query the data in a particular way, since to do so would risk circumvention of IPA.[79] Such difficulties can arise also in conjunction with foreign intelligence liaison partners.

- Similar problems have arisen in the domestic context, for example in the context of the fight against Covid during which it came as a revelation to some UKIC personnel to see how easily other government departments, subject only to normal data protection requirements, could retain and process bulk personal data.

- BPDs are an essential part of researching and developing AI capabilities, tasks often performed with commercial partners. The training of algorithms to be as fair and accurate as possible needs a wide range of training data, and the ability rapidly to substitute one set for another in a process of trial and error. Even a temporary inability to use commonplace datasets, freely available to commercial partners, complicates and lengthens these processes.

3.34. Some of the obstacles to cooperation that are posed by lengthy authorisation processes and complex handing and recording requirements are more indirect.

- One such problem is the issue of ***cover***. In order to protect a sensitive relationship with a data provider, it is sometimes essential to avoid overtly disclosing intelligence service involvement beyond those with a need to

[79] This is a risk to which UKIC lawyers are, in my experience, well-attuned.

know. When an intelligence service has to require the data provider to implement BPD safeguards that only apply to the intelligence services, the ability to maintain this cover is jeopardised.

- A second problem is the ***flagging appetite*** of data partners to cooperate with UKIC when to do so means applying not only data protection law but the Part 7 safeguards. The Review team was told that this level of governance makes UKIC unappealing partners, in comparison to almost everyone else to whom none of this applies.

- Thirdly, the bureaucratic processes around the use of BPDs impact on ***recruitment*** **and** ***retention of talent***. The Review team was told that bright data scientists – a scarce and desirable category of worker – are baffled and frustrated by what may strike them as pointless impediments, not found anywhere else, notably the need to spend months obtaining warrantry for standard open-source training data.

3.35. Further difficulties are caused by the need to adapt ***commercially available technology infrastructure***. MI5, in particular, has suffered numerous problems with its legacy, on-premises, organically grown IT estate.[80] Yet the obvious alternative – acquiring commercial, off-the-shelf products to store and hold BPDs – is complicated by the fact that this infrastructure is configured to comply with the standard safeguards of the DPA or UK GDPR, but not with the additional and unique requirements of Part 7. Limiting the application of the Part 7 requirements would provide increased flexibility to use datasets that sit outside MI5's estate.

3.36. A final disadvantage of compliance with the Part 7 requirements is its ***opportunity cost***. The number of BPDs held by UKIC is growing rapidly, with huge potential for further growth. Significant numbers of officials already devote their efforts to directly delivering BPD authorisations, or to supporting BPD policies. A lighter regime for some BPDs could allow part of this resource to be either redeployed or used to secure the authorisation of a greater volume of BPDs. Similarly, part of the engineering resource required to adapt commercially available products to store and hold BPDs could be used for other pressing tasks.

3.37. Turning to the specific requirements of Part 7, the issues identified by UKIC to the Review team were as follows.

[80] See the IPT's recent *TechEn* judgment in *Liberty and Privacy International v Security Service* [2023] UKIPTrib1: Annex 4 to this Report at §§5-9.

3.38. The first set of issues relates to ***protected and sensitive data***.[81] UKIC is barred from retaining and examining under a class warrant BPDs which include protected data (broadly defined in s203), health records or sensitive personal data, or which raise novel and contentious issues.[82] In consequence, prior to authorising retention, intelligence services must analyse every BPD (often manually) to ascertain whether any of those factors are present. The corresponding requirements in the BPD Code of Practice (6.2) flow directly from the IPA.

3.39. When seeking a specific warrant, the application must include a description of the BPD[83] and the Agency must explain why it is prevented from using a class warrant when applying for a specific warrant.[84] The corresponding requirements in the Code of Practice (4.24) flow from this and require a detailed explanation of the nature and extent of the material in question to be provided in the application.

3.40. Where it is assessed that a dataset contains protected data, there are requirements to provide as much detail as practically possible about the nature and type of data and any other factors that may be relevant when assessing the level of intrusiveness of the protected data.[85]

3.41. Where a dataset is organised and easily searchable, these tasks may not be difficult. However, other datasets of interest to UKIC are large, unstructured, and/or in a foreign language: for example data relating to a hostile state, or text from billions of pages from the open web, used in industry and academia as standard sources for the training of models. Some datasets are quite varied, and examining one part of the dataset does not necessarily give a good indication of the data as a whole; a thorough and time-consuming examination period would therefore be necessary, if it were feasible to examine it for protected data at all.

3.42. The second issue relates to ***access and storage***. The assumption of both the IPA and the BPD Code of Practice is that BPDs are highly sensitive material, requiring secure storage.[86] This does not recognise the variety of datasets that fall within the broad definition of BPD in IPA s199. Access requirements can impede cooperation with third parties who do not have staff cleared to the necessary level, making it impossible for example to use staff from a commercial partner to

---

81 See, generally, IPA ss26, 202, 203, 205, 207, 221, 222; Code of Practice 4.13-4.18, 4.24, 4.48, 6.4, 7.15-7.20, 7.21-7.24, 7.25-7.29.

82 IPA s202.

83 IPA s205(4)(a).

84 IPA ss205(4)(a), 205(5).

85 IPA s207; Code of Practice 4.48.

86 IPA ss204(3)(d), 205(6)(d); Code of Practice 7.3, 7.5.

help prepare a commercial dataset for ingestion into UKIC systems. Storage requirements can make it difficult to work at scale with data outside the estate.

3.43. The third issue relates to ***examination safeguards***. To be able to meet the requirement for examination standards[87] it is usually necessary to build a specific system for examining BPD. From that point, data needs to be organised ready for ingestion, often requiring a lot of highly skilled resource and creating a pinch point in the system. This requirement makes it difficult to make use of other commercial systems that have not been specifically designed to comply with Part 7.

3.44. The fourth issue relates to ***selection for examination***. Part 7 requires arrangements to be in force for securing that the selection of data for examination is necessary and proportionate in all the circumstances.[88] This requires a Justification Record to be completed, in which the necessity and proportionality case for accessing data is recorded. The introduction of role and task-based Justification Records remove the need for a necessity and proportionality case to be entered on every occasion that users work with a piece of data, but even this more strategic approach requires vast numbers of highly duplicative records to be prepared. Some uses of BPDs are repetitive in nature with a necessity and proportionality case that does not change over time, meaning that this can become little more than a cut-and-paste exercise that provides no meaningful additional protection for individual privacy rights.

3.45. The fifth, and least problematic, issue is the ***double lock***.[89] UKIC described the system for authorisation by the Secretary of State and approval by a Judicial Commissioner to be '*reasonably efficient*', but made the point that meeting the requirement for authorisation touches on many of the issues above.

BPD Issue 1: New Regime for Low/No Datasets

The proposal

3.46. As flagged in general terms in the Home Office Report, and on the basis of the operational experience of Part 7 detailed above, UKIC through the Home Office put to us a joint proposal, which developed during the course of the Review, to exempt some categories of BPDs from the full rigour of Part 7.

87 IPA s 221; Code of Practice 7.7, 7.8, 7.57.

88 IPA s221(1)(b).

89 IPA ss204, 205; Code of Practice chapter 5.

3.47. The essence of that proposal is to introduce an alternative statutory regime for the retention and examination of BPDs containing data in respect of which there is assessed to be a low or no expectation of privacy ('*low/no datasets'*), thus reducing significantly the time needed to authorise the use of such a BPD.

3.48. To assess whether a dataset is a low/no dataset, UKIC proposes to adopt a test that is defined by reference to the reasonable expectation of privacy in respect of the dataset, which it describes as the jurisprudential touchstone for the engagement of the privacy right in Article 8 of the ECHR. This seems to me broadly correct. Though a reasonable expectation of privacy is not necessarily conclusive of the issue,[90] additional legal assurance will be provided by the existence of safeguards (even if less extensive than those applicable under the existing Part 7) relating to low/no datasets.

3.49. Four principles are suggested by UKIC to be relevant to the expectation-based test:

- ***nature of the data***: the extent to which the nature of the data is such that an individual to whom the data relates would be considered to have a reasonable expectation of privacy;[91]

- ***data subject***: the extent to which there is evidence (i) that the data has been manifestly made public by the data subjects, or (ii) that the data subjects have consented for the data to be made public;

- ***publication***: the extent to which the data has been published subject to editorial control and/or the application of professional standards, and how widely known the dataset is; and

- ***use (or further use)***: the extent to which data has been used already in the public domain such that further use by UKIC for the purpose of its functions is unlikely to lead to further intrusion.

3.50. Discussions initially focussed on whether it would be enough for a dataset to satisfy any one of these criteria for it to qualify as a low/no dataset. Such a solution would be hard to reconcile with the fact that the criteria are expressed as variables rather than pass/fail tests. More substantively, the application of an '*any one criterion*' principle to hard cases could produce unjust results. Imagine a case in which a trove of highly sensitive personal data is hacked or leaked, and

---

90 *Bărbulescu v. Romania* (ECtHR, 2017) §73; see also *Campbell v MGN* [2004] UKHL 22, per Lord Nicholls at §21; *Bloomberg LP v ZXC* [2022] UKSC 5, §44ff.

91 Particularly relevant here are the concepts of protected data (IPA s203) and information of particular sensitivity (IPA s2(2)(5)).

finds its way on to a little-known corner of the dark web without its subjects' consent.[92] In such a case the public availability of the data (criterion 4) would militate in favour of a low/no classification. But other factors point in the opposite direction: the personal nature of the data (criterion 1), the absence of consent (criterion 2), the fact that it was dumped rather than curated (criterion 3), and the fact that it was not widely known (criterion 3). Rather than simply apply criterion (4), fairness might be thought to require the decision-maker to weigh the extent to which each principle is satisfied in order to reach a fair assessment in the round.

3.51. Two additional factors that seemed to me of possible relevance to the assessment are the ***anticipated use of the data***[93] and the ***location of the persons whose data is in issue***.[94] UKIC did not however seek to present a developed case to me on either of these factors, so I say no more about them.

3.52. Focus on potential hard cases should not obscure the fact that many decisions to classify a BPD as low/no are likely to be relatively straightforward. A non-exhaustive list of the types of dataset falling into the low-no category is as follows: news articles, academic papers, public and official records, online encyclopaedias audiobooks and podcasts, content derived from online video sharing platforms, publicly available information about public bodies, corporate registry/trade data, and internet infrastructure and operating data. MI5 and MI6 estimate that roughly 20% of their current BPD holdings would fall into the low/no category. For GCHQ this figure is estimated to be nearer 8%.[95]

3.53. Under the proposal, the following requirements of the Part 7 regime would be dispensed with or reduced:

- The requirement to thoroughly ***pre-examine*** and ***technically assess*** the data for protected/sensitive data. Instead, an assessment of the nature of the data would be made, based in most cases on existing publicly available

[92] Little imagination is in fact needed: data from the Ashley Madison site, which was supposed to enable extra-marital affairs, was leaked in 2015 and a link posted to it from a site on the dark web. The data included names, home addresses, search history and credit card transaction records. Other well-known leaks of bulk personal data are the Enron Corpus of emails and the Panama Papers.

[93] It seemed to the Review team that the use of data for training models might be a factor pointing towards a lower level of oversight, bearing in mind the nature of this process as described at 3.11 above. The point was however not pressed before us.

[94] I refer to location rather than nationality because in relation to bulk powers the scheme of the IPA is to accord certain additional safeguards to people in the British Islands (ss152(4), 193(4), 221(3)) but not to citizens of the UK or anywhere else. The sort of foreign database in respect of which the strongest case could be made for unhindered access (e.g. hypothetically, lists of soldiers or intelligence officers serving states engaged in hostile activity) may however already be subject to unhindered access, since a BPD will not fall within Part 7 if the majority of individuals on it may be of interest to UKIC: s199(1)(b).

[95] If authorisation becomes significantly easier via the low/no route, it is possible that the proportion of low/no datasets will increase well beyond these figures.

information about the dataset. It is acknowledged that some datasets may require additional examination (such as a proportionate dip sampling of the data) to provide assurance as to the nature of the data and whether, and to what extent, it might contain data of particular sensitivity.

- The requirement for ***Justification Records***, i.e. the need for a demonstrable necessity and proportionality consideration at the point of the selection of any data for examination in order to fulfil the obligations under s.221(1)(b). I was told that lifting this administrative burden would make it easier to organise and exploit data on commercial systems.
- The requirement to complete a very detailed ***BPD Internal Authorisation form***, engage legal and policy teams, determine and draft a class or specific new warrant and obtain ***external double-locked authorisation***. Instead, it is proposed that a simple Internal Approval Form will be completed by the analyst and approval granted internally by a Senior Manager outside the applicant's line management chain, where practicable.
- The requirement to ***store data*** on a locked-down platform which meets specific Retention, Review and Disposal (**RRD**) requirements, which either requires a bespoke platform to be created, or data to be input into already existing highly locked down systems. A DPA-style requirement, for example to ensure '*appropriate security of personal data*', would be substituted.

3.54. The mechanism proposed for achieving these goals is to amend IPA Part 7 so as to exclude low/no datasets from its authorisation regime and substitute a lighter set of safeguards. Data included in the low/no category could be authorised internally, would not require examination safeguards and would have more flexible storage and access requirements.

Discussion

3.55. I approached the UKIC proposal with a high degree of caution, and a good many questions. It is important to build on the success of the IPA by retaining and if possible enhancing public consent for the use of intrusive powers. Against a background of increasing and more sophisticated use of BPDs, it can be argued that tighter regulation, not deregulation, is the appropriate direction of travel.[96] Maximum value must also be obtained from the streamlining of existing procedures. The Review team quizzed the intelligence services for some time about their processes for achieving this. It is plainly sensible to realise the potential for cutting unnecessary bureaucracy under the existing regime before petitioning for the relaxation of statutory protections.

[96] This was a point emphasised by Liberty in its consultation response at §5, and by Privacy International at §2.3.1.

3.56. I have decided however to support the proposed change, in the form that I have outlined it above and on the conditions outlined below, for the following reasons.

3.57. First, ***the deregulatory effect of the proposed change is relatively minor.***

- It would apply only to a small minority of the BPDs currently authorised, and only to those in respect of which the level of intrusion into privacy is at its lowest.

- Low/no datasets that UKIC wished to retain and examine would still be subject not only to the data protection requirements under DPA Part 4 but to an additional authorisation requirement, with associated safeguards, that is unique to UKIC and not imposed on any other users of such datasets.

- There is no proposal to apply the change to other BPDs, or to dilute the regimes applicable to the potentially more intrusive Part 6 bulk powers reserved to UKIC.

3.58. Secondly, although the Review team was not in a position to conduct a full comparative analysis, there appears to be ***no international consensus for applying a regime as strict as IPA Part 7*** to BPDs in respect of which there is a low or no expectation of privacy.

- The ***United States*** Department of Defense (**DoD**) official policies give DoD components and in particular DoD intelligence organisations broad latitude to use publicly available information for these organisations' authorised mission and functions, without external review or oversight.

- In ***Canada***, '*publicly available datasets*' (an undefined concept but one that is understood to be broader than datasets in respect of which there is a reasonable expectation of privacy) are not subject to the same controls as other datasets in the hands of the intelligence services.[97]

- In ***Australia***, a comprehensive review of the law governing intelligence summarised the relevant frameworks in Canada, New Zealand and the UK, noting their partial application and the marked differences between them, before rejecting calls for primary legislation in Australia to govern the

[97] C. Forcese and L. West, *Squaring the Constitutional Circle with CSIS Datasets*, Intrepid podcast, 27 April 2019; C. Forcese and L. West, National Security Law (2021), pp 423-430. Note however the enhanced protection given by Canadian law to the data of Canadian citizens.

collection, retention and examination of bulk datasets, even by intelligence services that are exempt from the Privacy Act.[98]

3.59. Thirdly, and importantly, ***the operational arguments for the proposed deregulation are compelling***. These are summarised at 3.27-3.45 above. They were backed by written and oral evidence to the Review from all three intelligence services, including from those who were engaged at first-hand in intelligence operations at home and abroad. The Review team learned of occasions when it had proved impossible to exploit a window of opportunity because of delays in the authorisation of relatively innocuous datasets, and of multiple instances in which necessary cooperation with commercial partners, intelligence partners and other government departments was impeded by an inability to share and exploit information with the speed and flexibility that was available to their counterparties. Described in the bland and unspecific terms appropriate to an unclassified report, such incidents might seem to some a price worth paying for a regulatory regime that is highly protective of certain individual rights (notably, the right to privacy). In the real world, however, such impediments have the potential to affect the progress of a war, retard the development of effective new capabilities and even, in the long run, to affect the safety of the UK and the integrity of the democracy on which all our rights depend.

3.60. Fourthly, and more generally, there is the ***threat context***.[99] The weight of intelligence work, both at home and abroad, is tilting away from the alarming but often unsophisticated terrorist threat that preoccupied the West in the first two decades of the century towards what looks uncomfortably like a slow-motion struggle between states for global supremacy. There is a major war in Europe, in which UK interests are engaged. Further afield, the UK and its close allies are matched against illiberal regimes which seek by every means possible to harness technology and intelligence with the aim of rewriting the global order. Meanwhile at home, organised crime, fraud and child sexual exploitation test the abilities of LE to deal with them. The value of BPDs for identifying, enriching and moving against intelligence targets is increasing in both absolute and relative terms. We must not betray our values; but neither should we be unnecessarily cautious in defending them.

---

98 Dennis Richardson AC, Comprehensive Review of the Legal Framework of the National Intelligence Community (2020), vol. 3 (Information, Technology, Powers and Oversight), 34.40-34.48, 34.107-34.108, 34.111, 34.121-34.128. The Review noted however that facts may change over time, and that the issue of whether to introduce statutory controls should be reconsidered in future Independent Intelligence Reviews: Recommendation 141.

99 See 2.4-2.8 above.

3.61. As to ***safeguards***, a Code of Practice will have to make provision for the conduct of the initial examination and for the internal authorisation process applicable to low/no BPDs. It is accepted by UKIC that standards will need to be specified in respect of storage, access and examination, handling, retention, dissemination, deletion and record-keeping – the latter being important to inform both renewal applications (which would be made annually, if my recommendation under BPD issue 3 is accepted) and the regular IPCO inspections of Agency data holdings. Procedures will be needed to enable low/no authorisations to be revisited in the light of any potentially material discoveries, for example of sensitive personal data, and to require low/no authorisations to be cancelled if the criteria for them are no longer satisfied.[100] After-the-event oversight by IPCO will remain.

3.62. A significant statutory safeguard which I would add to the list is a requirement of ***prior approval by a JC*.**[101] This would be less of a burden than it may sound. The sole purpose of prior approval would be to certify that the relevant Agency had correctly concluded that the low/no condition was satisfied, applying the criteria described at 3.49-3.50 above. There would be no requirement to satisfy the JC that a full search had been performed for protected data, sensitive personal data and so on; nor to satisfy the JC in advance of the arrangements made for access and storage and examination safeguards. It would be a confined exercise, well within the expertise of a senior judge and requiring nothing from an Agency other than a reasoned statement of its justification for placing a BPD in the low/no category.

3.63. Things could be simplified still further by inviting the Secretary of State to authorise and JCs to approve ***classes of low/no BPDs*** to which, once approved, intelligence services could allocate datasets without further fuss.[102] BPDs determined by UKIC to fall within an approved class would simply be notified to a JC.[103] Any BPD not falling within an approved class would require individual JC approval on the reduced basis described at 3.62 above (or the authorisation and approval of a new class to which it, and similar BPDs, could be allocated).

3.64. This arrangement would have the following advantages:

---

100 This would not of course prevent a Part 7 warrant from being obtained if it was still wished to make use of the BPD.

101 There are precedents in the IPA both for JCs to grant approval (the classic double lock) and for the IPC to grant authorisations (s60A).

102 On the analogy of IPA s204. A rough idea of what the classes might look like is provided by the categories identified by the intelligence services themselves at 3.52 above. To the extent necessary, handling arrangements for BPDs falling within each class could be authorised and approved at the same time.

103 Compare the procedure for notification of criminal conduct authorisations to a JC under RIPA s32B, inserted by the Covert Human Intelligence Sources (Criminal Conduct) Act 2021 s6.

- ***Operational speed and flexibility***:
    - Once classes had been authorised and approved under the double lock procedure, most if not all low/no BPDs could be added to them straightaway, without any process save simple notification.
    - Any BPDs falling outside a class but determined to constitute a low/no BPD could be approved as such by a JC without further formality within a few days or even, if urgent, once use of the BPD had begun.[104]
- ***Political accountability:*** the Secretary of State would have responsibility for authorising the low/no classes.
- ***Holding intelligence services to high standards:*** **t**he knowledge that UKIC's statement of justification for placing a BPD in the low/no category (or one of the agreed classes) would be scrutinised by a JC should incentivise those preparing it to have regard to all relevant factors.
- ***Assisting after-the-event review:*** experience in drawing up the classes, and determining any specific applications, would help IPCO inspectors in their after-the-event review, and JCs in drawing up any necessary guidance on how the low/no criteria should be applied in the future.
- ***Reduced legal risk***: the optimum safeguard of prior judicial approval[105] would be satisfied (whether on a class or specific basis) in every case of a decision to place a BPD in the low/no category.
- ***Public confidence:*** public, and Parliament, would have an assurance that the crucial borderline between normal and low/no BPDs will be patrolled externally and not simply by intelligence services which, however fairly they might approach the issue, will always have an interest in placing a BPD on the low/no side of the line.

3.65. Though the low/no idea was originally put to me on the basis of self-authorisation by the intelligence services, it would in my view be greatly improved by a mechanism such as that outlined in 3.62-3.64 above. On that basis, I am happy to approve it.

---

104 By means of an urgency procedure on the analogy of IPA s209, whereby a BPD could be retained and examined in advance approval by a JC.

105 *R (Liberty) v SSHD* [2020] 1 WLR 243 at §§ 33, 149-150, 161, 218, 227, 240.

3.66. ***I recommend that IPA Part 7 should be amended to recognise a new category of BPDs in respect of which there is a low or no expectation of privacy, to which a distinct and less onerous set of safeguards should apply.***

3.67. ***Provision should be made for low/no classes to be authorised and approved via the double lock, and for any proposed low/no BPD falling outside the terms of a class to be approved by a JC as meeting the low/no criteria.***

BPD Issue 2: Warrant Duration

3.68. BPD warrants cease to have effect six months after they were issued, unless they have already been renewed or cancelled.[106]

3.69. As flagged in the Home Office Report and in the List of Specific Topics, the Home Office (on behalf of the intelligence services) asked me to consider a proposal for this duration to be extended to 12 months.

3.70. Self-evidently, a doubling of warrant duration will reduce the administrative effort that it is necessary to devote to the warrantry of BPDs. That would be desirable if it can be achieved without a material weakening of safeguards. On that issue, the following points were made to me:

- The intelligence value of BPDs tends to be more ***static and predictable*** than that of warrants targeting the acquisition of communications. It is less likely, therefore, that the benefit of a BPD will have disappeared or significantly diminished by the time that the first 6-monthly renewal application will have to be contemplated, often after as little as 3 months.

- BPD data is often used to support ***long-term strategic intelligence activities*** rather than short-term tactical actions. The Secretary of State will be better equipped to decide after 12 months than after 6 on the necessity and proportionality of a warrant renewal.

- While ***bulk interception and bulk EI warrants*** also cease to have effect after 6 months,[107] they are inherently more intrusive by nature; and in any event, it is usual for equivalent data obtained using those powers to be

[106] IPA s213

[107] IPA ss143, 213.

subject to a maximum retention period of at least 12 months without additional approval.[108]

3.71. I asked for the statistics relating to warrant renewals and was told that no application to renew a BPD authorisation has ever been refused to any of the three intelligence services by either the Secretary of State or a JC. It is difficult to argue, therefore, that a 12-month renewal period would allow significant numbers of BPDs to run on in circumstances where renewal is likely to have been refused.

3.72. It also occurred to me to wonder whether the approach of a renewal deadline might have the benefit of encouraging intelligence services not to seek the renewal of redundant or only marginally useful BPDs. An extension of the renewal deadline from 6 to 12 months could, were no other factors in play, delay that benefit.[109] However, other factors *are* in play: each Agency is under an independent obligation regularly to review the operational and legal justification for the continued retention, examination and use of each of its BPDs, at intervals agreed with the Secretary of State;[110] and the Secretary of State may cancel a BPD at any time, requiring the intelligence services to '*keep their BPD warrants under continuous review and … notify the Secretary of State if they assess that a warrant is no longer necessary*'.[111]

3.73. IPCO's latest annual report notes a satisfactory level of compliance by MI5 and GCHQ with the rules on BPDs, including the review and deletion of warranted material.[112] While MI6 was criticised for failing to delete some legacy files that may constitute BPD, it seems that these files were never warranted with the consequence that warrant duration was not a relevant factor.[113]

3.74. The consultation responses did not address this proposal.

3.75. The advantages of the proposal seem to me to outweigh any disadvantages and accordingly ***I recommend that IPA s213 be amended to provide that BPD***

---

108 Maximum retention periods for different categories of data vary, and '*should not normally be longer than two years*': Interception of Communications Code of Practice (December 2022), 9.24; EI Code of Practice (March 2018), 9.31.

109 Though only in relation to BPDs which are not being used, or productively used.

110 BPD Code of Practice, 7.53.

111 BPD Code of Practice, 5.58-5.59. The Review team was informed that GCHQ has proactively cancelled 11 BPD warrants (4 class and 7 specific) before their expiry since the IPA came into force, 5 of them because the dataset(s) had not delivered the expected value and 6 because it was no longer necessary to retain the dataset(s).

112 IPCO 2021 Annual Report, March 2023, 8.27-8.28, 8.34; 10.28-10.30.

113 *Ibid.*, 9.22.

warrants cease to have effect 12 months after they were issued, unless they have already been renewed or cancelled.

BPD Issue 3: Delegation

3.76. The IPA contains numerous provisions allowing for functions to be performed by a Crown servant (i.e., in this context, an official of the intelligence services) on behalf of an Agency Head (i.e. the Director General of MI5, Chief of MI6 and Director of GCHQ). A number of sections are, however, drafted without any explicit provision for delegation to another officer acting on the Agency Head's behalf. It has been suggested that those provisions might be interpreted as requiring the Agency Head to exercise those functions personally.

3.77. The provisions in question were spelled out neither in the Home Office Report nor in my Terms of Reference. I was able to list the provisions in the List of Specific Topics, but the subject attracted no specific interest in the consultation.

3.78. The first set of provisions in question are:

- a requirement on Agency Heads to consider whether specific BPDs consist of or include protected data, health records or sensitive personal data, and whether novel or contentious issues are raised;[114]

- a requirement on Agency Heads to consider whether specific BPDs contain or are likely to contain health records;[115] and

- a requirement on Agency Heads to conduct elements of the initial examination of specific datasets, e.g. for the purposes of determining whether they are BPDs and whether they should be retained.[116]

3.79. Each of these tasks is of a routine nature, quite capable of performance by Agency officials with the relevant experience and expertise. It is hard to conceive that Parliament could possibly have intended them to be performed personally by Agency Heads. Furthermore, the Agency Head would remain accountable for the exercise of each of these functions by Crown servants, and BPD warrants would still remain subject to the double lock applied by Secretary of State and JC. I endorse the proposed amendments.

---

114 IPA s202(1)(2)(3).
115 IPA s206(4)(5).
116 IPA s220(1)(2).

3.80. A similar proposal is made in relation to three other sections of the IPA, providing respectively for:

- Agency Heads so far as reasonably practicable to secure that where a JC refuses to approve the decision to issue an urgent warrant, anything being done in reliance on the warrant stops as soon as possible;[117]

- Agency Heads to apply, after the non-renewal or cancellation of a BPD warrant, for a further period of up to 3 months in which the material subject to the BPD can continue to be retained and examined;[118] and

- Agency Heads to apply for a direction that BPDs obtained pursuant to any other authorisation issued or given under the IPA, with the exception of a bulk acquisition warrant, be retained and examined under the Part 7 regime.[119]

3.81. There is no reason why the second and third of those functions should be restricted to Agency Heads. While the making of applications for warrants and directions is an important function, the applications with which IPA ss219 and 225 are concerned are of a lesser order than the main applications for class and general BPD warrants which may be made by '*the head of an intelligence service, or a person acting on his or her behalf*'.[120] I see no basis for applying any different and more restrictive formulation here.

3.82. The first of those functions is, however, of a quite different nature. It places an obligation on Agency Heads to secure that an urgent warrant which has been refused judicial approval should not be acted upon.[121] This is a basic safeguard against conduct which, if it were ever to take place, would be seriously unlawful. This burden is not excessive, for the obligation is expressed only as being to *secure* that the relevant Agency respects the ruling of the JC. It seems to me entirely appropriate that to mark its importance, that obligation should be placed personally on Agency Heads.

---

117 IPA s210(2).

118 IPA s219(2).

119 IPA s225(3).

120 IPA ss204(1), 205(1).

121 The issue may arise because, under the urgency procedure in IPA s209, JC approval may be sought after a warrant has been issued.

3.83. Accordingly, ***I recommend that IPA ss202, 206, 215, 219 and 220 (but not s210) be amended so as to provide explicitly that the functions with which they are concerned may be exercised by a Crown servant on behalf of an Agency Head.***

4. INTERNET CONNECTION RECORDS

Description

4.1. ICRs are a form of CD, succinctly described in the relevant Code of Practice as '*a record of an event held by a telecommunications operator about the service to which a customer has connected on the internet*'.[122] They contain rich data about access to internet services, but no content information about the service activity itself.[123]

4.2. In one sense, ICRs are simply the internet equivalent of telephone CD logs. However, as the internet is the medium in which we increasingly live our interior as well as our outward lives, a person's browsing history can reveal appreciably more about them than their telephony records. The generation, collection and use of ICRs accordingly was, and remains, controversial with privacy campaigners. This is reflected in the IPA, which places additional restrictions on ICRs by comparison to basic telephony CD.[124]

4.3. Collecting and using ICRs is not a straightforward business. It requires telecoms operators to collect and store the correct network records, and investigators to make good-quality queries and inferences from those records. As internet usage shifts to mobile phones, connecting to the internet through home and public WiFi and 3G/4G/5G, and as network operators continually change the internal architectures of their networks, the difficulties of exploiting ICRs increase.

4.4. No doubt for such reasons, progress towards the operationalisation of ICRs has been slow. A trial has shown that ICRs are a valuable investigative tool but that they take considerable effort, cost, and skilled resource to implement well.[125] In addition, it is often suggested that customers will increasingly be able to frustrate

---

122 CD Code of Practice (November 2018), 2.74: see also the legal definition in IPA s62(7). Prof Peter Sommer noted what he called the '*ad hoc quality*' of the concept, which he suggested would require bespoke tools to be crafted by TOs, and would place a particular burden on OCDA in determining that content is not inadvertently captured: consultation response at §24. His full response can be found at http://www.pmsommer.com/IPA_Review_2023_Sommer.pdf.

123 Thus, in practical terms, ICRs can tell investigators that Device A connected to Service B at 12:07:12, sent 100 kB of data and received 200 kB of data, but cannot identify the content that was posted or files that were downloaded.

124 ICRs may not be granted to local authorities (s62(A1)), can only be obtained for the limited purposes spelled out in s62(3)(4) and (5), and are subject to the authorisation levels appropriate to events data (CD Code of Practice 2.35, 9.1).

125 As Professor Peter Sommer put it in his consultation response at §26: '*The [ICR] is a concept developed to meet declared law enforcement investigatory needs but which turns out to be extremely difficult to implement in practice.*' Graham Smith also referred to the practical difficulties with implementation at §24 of his response, including the possibility that TOs would have to create specialist tools for the acquisition of ICRs.

the collection of ICRs by various means which allow them to browse the internet without revealing their IP addresses. One telecommunications operator (**TO**) described ICRs to the Review team as '*a gold-plated solution which will take a long time to generate*'. The service is now being rolled out in a more scalable model within the National Communications Data Service (**NCDS**). It is described in the Home Office Report as having shown significant operational benefit, but is still at an early stage of implementation.

4.5. I understand it to remain the case, as it was when AQOT was published in 2015, that no other Five Eyes or European country provides for the compulsory retention of ICRs (or weblogs, as they were previously known).[126]

Operational value

4.6. ICRs are generally recognised to have the potential to do three things:

- attribute ***communications*** with a known internet service to an individual device (and hence user);
- identify the ***communications sites*** used by a subject of interest (enabling those sites to be approached with requests for CD and content); and
- gather intelligence or evidence on ***web-browsing activity***, both on sites suggestive of criminality and more generally.

4.7. The first of those capabilities is of great potential value in target discovery: for example, tracking down the users of sites used for child sexual abuse and exploitation.

4.8. The second and third capabilities, which serve to enrich knowledge of a target (target development), can be achieved also through targeted interception. This however is a highly intrusive power, reserved to a limited range of public authorities that includes UKIC and the NCA but not general policing. ICRs promise the advantage of giving LE bodies a summary view of a subject's internet activity, without interception and without the privacy intrusion associated with content collection.

---

126 On the troubled pre-history of ICRs see, generally, AQOT §§14.23-14.38. I recorded at §14.33 that I had not been presented with a properly worked-up case for ICRs. An Operational Case for the retention of ICR records was produced later in 2015 and this informed the debates in Parliament. It made no mention of the proposed extra condition discussed below.

ICR Issue: Facilitating Target Discovery

4.9. I was asked to consider only one, relatively confined, issue relating to ICRs. It concerns the scope of Condition A in IPA s62: the first of three alternative conditions that must be satisfied before authorisation can be granted to obtain ICRs, and the only one that enables target discovery.[127]

4.10. Condition A in its current form requires it to be necessary, for a given statutory purpose:

> '… to obtain the data to identify which person or apparatus is using an internet service where –
>
> (a) the service and time of use are already known, but
>
> (b) the identity of the person or apparatus using the service is not known'.

4.11. The concern relates to the requirement that the '*time of use*' of an internet service must be '*already known*'. This appears to imply that the authorities must know that a given IP address was used to access the service at a given moment. That is a possible scenario if for example a server has been seized or if web-access logs have been provided to an investigation, voluntarily or under compulsion. The purpose served by an ICR would therefore be to attribute that address to a particular device and thus identify a suspect. Condition A will not however be satisfied if the '*time of use*' is unknown. Thus, it allows devices (and hence potentially users) which are already known to have contacted a site at a particular time to be *identified*; but it does not permit new targets to be *detected* by observing visits to internet platforms which, alone or in combination, are strongly indicative of serious criminal behaviour or a national security threat. This would require legislative change, most obviously by the introduction of an extra condition.[128]

4.12. The operational case for the extra condition is supported by the following two hypothetical examples presented to me by GCHQ, relating in one case to cybercrime and in the other to CSA. Both concern the detection of targets via their access to a combination of platforms. Having talked through them in detail at a

---

127 Conditions B and C (which are distinguished from each other by the purpose for which data is sought) require the target to be known, and allow information to be sought on their internet activity.

128 It might be possible to argue for a highly flexible interpretation of Condition A: if the '*time of use*' could be understood for example as a period of several months, Condition A might be used to detect previously unknown users of a service. But even if this interpretation were correct as a matter of law, which I strongly doubt, it would risk contributing to a situation in which the IPA, like RIPA before it, became '*incomprehensible to all but a tiny band of initiates*': AQOT, Executive Summary §35.

classified level, the Review team concluded that they offer a realistic picture of how the extra condition could be used.

- ***High-harm fraud*** often involves online behaviour that could be identified by ICRs. ICRs could be used, for example, to search for devices which were simultaneously connecting to legitimate banking applications and to malicious control points. Such behaviour could indicate that a financial fraud is in progress. Improved access to ICRs could enable the intelligence services to detect such activity more effectively and to inform LE colleagues of the identity of the potential fraudsters and of any associated organised crime groups. Flagging suspicious behaviour in that way can lead to action being taken to prevent criminals from defrauding their intended victims.

- ICRs could be used to identify ***high-risk CSA*** offenders, including those who both access multiple CSA platforms and have easy access to children. Records obtained by intelligence services of engagement in particular combinations of online behaviours could be shared with LE partners. They could assist them in prioritising their efforts against CSA, protecting children and bringing offenders to justice.

4.13. The Review team was also shown national security scenarios to which detection and identification from ICRs would make a large difference, but these are impossible to share publicly without damaging operations and capability.

4.14. The limitations on Condition A, and the value added by the proposed extra condition, are particularly evident in those very many cases where the web services that enable criminality are situated abroad – often in countries where cooperation with UK LE is limited or non-existent. UK users of a foreign-based internet service that spreads terrorist material, perpetrates fraud or sells child sexual abuse images can be apprehended using Condition A if the owner of that '*far-end*' service cooperates, or if the site is seized, the logs are inspected and the results passed on to UK LE: but this will often be impracticable. The proposed extra condition would have the important advantage of allowing UK users of such sites to be identified without access to the site logs.

Consultation

4.15. The Home Office Report alluded to this issue only in the broadest of terms. While the Terms of Reference mentioned the conditions restricting the usage of ICRs in IPA s62, and while the List of Specific Topics made express reference to s62(3) (Condition A), I was not able to invite comment on the precise proposal before

me (which evolved, in any event, during the course of the Review). Nonetheless, ICRs were the subject of comment in the consultation responses. Graham Smith emphasised Parliament's deliberate decision to impose a high bar before ICRs could be authorised, in light of the serious intrusion involved. He reminded us that '*it ought not to be assumed that operational benefit is of itself a reason to lower the bar*', and that '*Parliament would hardly have been prepared to grant the powers at all had it not been assured of the likelihood of operational benefit*'.[129]

4.16. It is all the more important, in these circumstances, that any proposed extra condition on the basis of which ICRs would be obtainable should receive proper pre-legislative scrutiny.

Discussion

4.17. Having weighed up the competing factors, my own view is that intelligence services should be empowered to use ICRs – subject to a range of appropriate safeguards – for the target-detection purposes outlined above. My reasons are, in summary, as follows:

- As the above examples show, ICRs have the capacity to make ***a decisive contribution*** to the prioritisation and pursuit of both national security and serious crime investigations.

- Their potential is particularly strong in relation to types of ***internet-enabled crime*** (such as CSA and online fraud) which are extremely common and yet whose perpetrators often go undetected. Successful OCGs employ a combination of tactics, including use of secure internet infrastructure in inaccessible jurisdictions, designed to thwart nationally-based LE agencies. It is appropriate that the most technically-capable agencies should be able to help LE detect and disrupt their activity.

- The ***safeguards*** attending ICRs are already extensive: as well as the limitations imposed by Conditions A-C they have included, since at least 2018:[130]

    - a limited range of purposes for which, and public authorities by which, ICR requests may be made;[131]

---

129 Graham Smith, consultation response §48.

130 IPA Part 3 was amended by The Data Retention and Acquisition Regulations 2018 following the 2016 judgment of the Court of Justice of the EU in the *Tele2 and Watson* case, as interpreted by the High Court in *R (Liberty) v SSHD* [2019] QB 481.

131 IPA s62.

- a requirement that data requests be authorised in advance by the IPC as necessary and proportionate for a specific investigation or operation;[132]

- detailed provisions governing the security, integrity, use and destruction of retained data;[133] and

- regular inspections by IPCO, summarised in its annual report.

- The ***intrusiveness*** of the proposed new target-detection power is arguably no greater than that of the target development powers in the existing Conditions B and C.

4.18. It would however be open to Parliament to require ***further safeguards***, to the extent that the nature of the proposed extra condition is thought to require them. I suggest that these should include:

- making the extra condition available ***only to UKIC***, at least in the first instance;[134] and

- limiting the purposes for which requests may be made to national ***security-related and serious crime purposes***.[135]

It would also be possible to make requests subject to the full double-lock procedure, but this would seem disproportionately burdensome for individual CD requests.

4.19. Accordingly, ***I recommend that a new condition be inserted into IPA s62 allowing UKIC to obtain ICRs, if so authorised by the IPC, when it is necessary and proportionate for a national security or serious crime investigation to detect persons or devices using specific internet services.***

---

132 IPA s60A: the power is delegated to the Office for Communications Data Authorisations (OCDA), which is under the control of the Investigatory Powers Commissioner. A 3-day authorisation may be granted for specified purposes without recourse to OCDA where there is an urgent need to acquire the data: IPA s61A, CD Code of Practice 5.28-5.40.

133 CD Code of Practice, s3.

134 Working arrangements, on the analogy of those that exist in other contexts, could facilitate the use of UKIC powers in the service of NCA or CTP in particular.

135 On the analogy of IPA s61(7), which is a pared-down version of the list of purposes in s60(7).

5. DATA RETENTION NOTICES

Description

5.1. The retention of CD is dealt with in Part 4 of the IPA. A DRN may be served by the Secretary of State on a TO, having taken specified matters into account. It may require the TO to retain relevant CD if that is judged necessary and proportionate for one or more purposes including the interests of national security, the prevention or detection of serious crime and the prevention of death or injury.[136] Decisions to give, vary or confirm a DRN must be approved by a JC.[137] TOs are required to comply with requirements or restrictions imposed by a DRN, and prohibited from disclosing the existence or contents of a DRN.[138] A DRN may relate to conduct and to persons outside the UK, but compliance with a DRN cannot be enforced by civil proceedings against persons outside the UK.[139]

5.2. The operational value of retained CD to LE is beyond question,[140] though a number of challenges to the '*general and indiscriminate*' retention of data have been successful before the EU's Court of Justice.[141]

5.3. CD relating to applications or services from other providers running over a TO's network, including both telephony roaming services and '*over the top*' (**OTT**) services such as Google search and Facebook, is described as third-party data. IPA s87(4) provides that a DRN may not require the retention of third-party data.

Consultation

5.4. The Home Office Report indicated somewhat elliptically that IPA s87(4) may need to be amended in the light of '*the introduction of a new technology*', evolving standards and business models and '*the introduction of new routing technologies*'. My Terms of Reference contained a reference to '*third-party data relating to the communications data retention regime*', but did not specify the changes that were

136 IPA ss87, 88.

137 IPA ss89, 91.

138 IPA s95.

139 IPA s97.

140 See AQOT at §§9.21-9.32, 9.43-9.47 and Annex 10.

141 The CJEU, in distinction to the more pragmatic approach of the ECtHR, has thus far taken '*a position of high principle that there can be no general retention of data other than where there is a grave and present risk to national security*': C. Vajda KC, 'Data Protection: Made in Europe and Exported Globally', UKAEL Annual Lecture, 19 January 2023. This rare difference of approach between the two senior European courts has been acknowledged by each of them: *Big Brother Watch v UK*, Chamber judgment of 13 September 2018, Opinion of Judges Pardalos and Eicke at §22 (a case subsequently referred to the Grand Chamber, judgment of 25 May 2021); Joined Cases C-793/19 and 794/19 *SpaceNet* EU:C:2022:702, §125.

under contemplation. The List of Specific Topics was slightly more forthcoming, referring to the Home Office Report and inviting comment on

- whether to address unintended consequences of s87(4) third party data definition, and
- the impact of future development in ways of working and technology on data retention capabilities.

The consultation responses did not address these points.

5.5. Nothing was said in the Home Office Report, my Terms of Reference or the List of Specific Topics about the proposed expansion of extraterritorial effect. This diminished the value of my consultation on this point, and points up the need for further consultation should it be decided to put these changes into a Bill.

DRN Issue 1: Inbound Roaming Data

5.6. A requirement on UK TOs to retain third-party data passing over their networks has been a contentious subject since at least the draft Communications Data Bill of 2012. Recognising that data retention requirements would be difficult to enforce extraterritorially, the draft Bill would have required UK TOs to store and disclose CD traversing their networks which related to services (for example email traffic) from other providers. The draft Bill attracted strong criticism from a parliamentary committee which said that it was *'too sweeping, and goes further than it need or should*'.[142] It split the coalition government, and was withdrawn.

5.7. The retention of third-party data remained controversial during the passage of the IPA. I had recommended in AQOT that there should be no question of requiring the retention of third party data until a compelling operational case for it had been made. Third party data retention met with strong opposition from domestic providers, and it was eventually ruled out by a government amendment to the Bill during its passage through the House of Lords. This became s 87(4) of the Act.

Home Office proposal

5.8. The proposal I am asked to consider is not to revisit the issue of principle but to restore the operational position as it stood at the time of the IPA by reversing what is anticipated to be a discrete but damaging unintended effect of s 87(4): its

[142] Draft Communications Data Bill Joint Committee First Report, November 2012, para 281. The issue of third party data was considered at paras 89-109 of the Report. See, further, AQOT at §§9.62-9.64.

possible application[143] in such a way as to prevent the retention of CD – including, potentially, ICRs – for so-called '*inbound roamers*' (users of a foreign SIM within the UK).[144]

5.9. Relevant here is the future growth of S8 Home Routing ('S8HR'), a new method for delivering international roaming services that will see 4G voice calls and messaging not being handled by the UK operator but being automatically routed via the home (i.e. in the case of inbound roamers, non-UK) networks over a dedicated IP link. For 5G services, an equivalent form of Home Routing will be implemented ('N9HR'). The effect of S8HR (and in due course N9HR) will be to deprive UK LE of material to which they have had access to date: namely, CD relating to voice calls and messaging.[145]

5.10. While a form of home routing has been part of the applicable standards since the days of 2G, I was told that it was only in 2020 through engagement with UK Mobile Network Operators (**MNOs**) that the consequences of s87(4) were identified. Few S8HR agreements have been implemented to date, but the number is predicted to increase markedly. The amendment of s87(4) is said to be necessary in order to ensure that a significant capability gap does not emerge.

Reaction of the Telecommunication Operators

5.11. The Review team had an opportunity to discuss the Home Office proposal with UK service providers. They disagreed with the premise of the Home Office's proposal – that the application of s87(4) to inbound roamers is unintended – and countered that '*the safeguards set out in s87(4) are vital and working exactly as intended*'.

5.12. The TOs did not claim that it would be technically impossible for them to retain the CD of inbound roamers in all circumstances. They did tell the Review team, however, that:

- The core part of the service is provided by the overseas operator, which is likely to have CD records (**CDRs**) for the voice traffic for its own billing purposes. Should the government wish these CDRs to be retained, it is open to the Secretary of State to serve a DRN on the overseas operator.

---

143 There is some legal uncertainty, acknowledged by the government, over the question of whether for the purposes of s87(4) the UK TO is a joint provider (with the foreign TO) of an inbound roaming telecommunications service.

144 Users of a UK SIM abroad, conversely, are known as '*outbound roamers*'.

145 Not the contents of the calls or messages, but the call logs, location data &c.

- The UK TO, by contrast, does not generate CDRs relating to the overseas operator's service. A retention obligation on the UK TO would require it to engage in intrusive bulk probing of the data traffic, in an attempt to extract the relevant signalling communications carried within the packet data – in effect, to generate pseudo-CDRs, which would not meet evidential standards. This process would be costly, could not be accommodated within existing data centres, would occupy engineers who could be more productively engaged elsewhere and would slow down the TOs commercially and technologically. Not even 100% reimbursement of costs incurred would compensate for these disadvantages.

- Even this bulk probing would not produce useful results if the overseas operator implemented transport encryption, which is readily achievable technically, and which encrypts the connection between the subscriber's user equipment and the overseas operator's infrastructure. While a UK TO might look to prohibit the overseas operator from doing this on a commercial basis, it was doubted whether a TO could realistically enforce such a clause against an overseas partner that wished to implement encryption.

5.13. Scepticism was also expressed about the likely value to LE of the pseudo-CDRs that UK TOs might be required to generate. They would not be of evidential quality; and it was suggested that inbound roamers who are criminally inclined might look to encrypted alternatives which are readily available without cost.

5.14. The TOs also voiced fears of a slippery slope, from this specific technology towards a general obligation to retain third-party data. They were curious to understand how an exception to s87(4) could be drafted that would not allow its use in other circumstances: for example, to require a TO to construct CDRs for a non-telephony OTT service such as WhatsApp, FaceTime or Skype, or new routing technologies.

5.15. Underlying the TOs' attitude to the Home Office proposal were more general preoccupations: a sense that imaginative but technically complex solutions arrived at by government were liable to prove slow or impossible to roll out; concern that lengthy response times (exacerbated by rapid staff turnover and consequent gaps in institutional memory) make it more difficult than it should be to engage in technical discussions with government; and a degree of frustration that UK TOs, while increasingly acting as '*dumb pipes*' for OTT services provided from elsewhere, were being expected to engage in ever more marginal attempts to extract intelligence value from those services, building – in the colourful phrase

of one of our interlocutors – '*surveillance networks with some consumer propositions on them*'.[146]

Home Office response

5.16. I put this reaction to the Home Office, which emphasised the difficulties that are likely to emerge and the importance of addressing them before the general rollout of S8HR and eventually N9HR. Officials accepted that utility would be likely to diminish in the long term as inbound roamers migrate to OTT services, but did not think this point had yet been reached. Their assessment was that DRNs would constitute value for money, and that to issue large numbers of DRNs to foreign operators would, in the absence of international agreements, be a complex and cumbersome business. They explained their reasons for considering that the risks of encryption being implemented by overseas operators were manageable. They emphasised, finally, that we were concerned here not with OTT services of which the UK TOs had no understanding, but with traditional telephony services delivered via S8HR, a facility to be put in place and maintained by TOs themselves.

Discussion

5.17. The frustrations of the UK TOs speak for themselves, and are entirely understandable. So, however, is the desire of LE to ensure that it can continue to obtain the call records of suspected criminals operating in the UK.

5.18. The question before me is not whether it is necessary or proportionate to grant a DRN in any individual case, but whether the *option* of a DRN should be available, for the purposes set out in s87, if the double lock can be satisfied. This would mean the Secretary of State considering a DRN to be necessary and proportionate in the individual case (having consulted the TO affected and taken into account the likely benefits, the likely number of users, the technical feasibility, the likely cost and any other effect of the DRN on the TO).[147] It will further require a JC to grant approval, applying the judicial review test but having considered the issue of privacy intrusion with '*a sufficient degree of care*'.[148]

5.19. I agree with the Home Office that inbound roaming is not directly comparable to the wider third-party data issue because roaming data has been traditionally available to LE, and because the TOs will play their part in making possible S8HR and N9HR.

---

146 These views echo those recorded in AQOT §§11.32-11.38.

147 IPA s88.

148 IPA s89.

5.20. I have no basis on which to express a view on the likely cost-benefit analysis of obtaining inbound roaming CD via such a DRN. No doubt the relevant factors will be closely considered when any application is made. I am clear however that the applicable procedures provide for the interests of TOs and their customers to be protected, and that in all the circumstances it would be wrong to deprive LE of the opportunity to seek a DRN for the purposes of obtaining CD to which, but for the advent of S8HR, they would continue to have ready access.

5.21. ***I recommend that IPA s87(4) be amended so as to allow DRNs to be applied for in relation to inbound roaming data.***

DRN Issue 2: Extraterritorial Effect

5.22. The Home Office asked me to consider the arguments for extending the extraterritorial effect of DRNs. As noted above, the duty to comply with a requirement or restriction imposed by a DRN already applies extraterritorially, but is enforceable by civil proceedings only against providers in the UK.[149] By way of comparison, the enforceability abroad of Technical Capability Notices (**TCNs**) depends on the nature of the Notice.[150]

5.23. No operational case has been developed by government for granting extraterritorial enforceability to the full range of TCNs. It is however possible to imagine situations in which, depending on the policy factors involved, there might be a national security or LE interest in enforcing DRNs internationally.[151]

5.24. The large US TOs have been historically opposed to the extension of extraterritorial jurisdiction. This was a sensitive issue in 2015, during the passage of the IPA because the issue was seen as linked to their support for the ground-breaking US-UK Data Access Agreement (**DAA**), which allows UK and US LE to request data held by telecommunications providers in each other's jurisdictions.[152]

5.25. There is, in addition, always likely to be a something of a mismatch between the claimed legal powers and the reality on the ground. Attempts to enforce abroad

149 IPA s97.

150 IPA ss255(9)-(11). TCNs relating to bulk CD and EI are enforceable only within the UK, whereas TCNs relating to targeted CD, targeted interception and bulk interception are enforceable (at least notionally) by civil proceedings against entities anywhere in the world.

151 One potential target of such enforcement might be the use of technologies that pass browsing traffic through proxy servers, threatening the capability of UK TOs to conduct IP address resolution (IPAR) and ICRs

152 Meta, Google and Microsoft separately volunteered to the Review team their experience of the operation of the DAA, which was illuminating but not strictly relevant to the scope of this Review.

face potentially insuperable problems; an enforcement power written into UK law can only be exercised on the territory of another State with its consent. Successful extraterritorial enforcement thus requires the cooperation of foreign courts and enforcement mechanisms, which will be forthcoming only if provided for by international agreement. It remains to be seen, therefore, whether extraterritorial enforcement is a realistic option even in those cases when it is permitted under UK law.

5.26. In AQOT I took a pragmatic approach to the issue of extraterritorial jurisdiction:

> 'I understand those who argue that extraterritorial application sets a bad example to other countries, and who question whether it will ever or could ever be successfully enforced. It is certainly an unsatisfactory substitute for a multilateral arrangement under which partner countries would agree to honour each other's properly warranted requests, which must surely be the long-term goal. But some service providers find it easier to assist if there is a legal power purporting to require them to do so; and despite the fact that extraterritorial enforcement has not yet been tried, the presence on the statute book of DRIPA 2014 s4 has been of some assistance in securing vital cooperation from service providers. On that pragmatic basis I suggest that it should remain in force, at least for the time being.'[153]

5.27. I would add that even if the foreign enforcement of a DRN is not permitted by international agreement, it might at least notionally be open to the UK to punish non-compliance by preventing the service in question from operating in the UK. This could however be difficult reputationally, depending on the profile of the service concerned, and could provoke retaliatory measures.

5.28. Whether to amend IPA s97 so as to make DRNs enforceable overseas is a policy question on which it would be wrong for me to suggest a definitive answer. The proposal could reasonably be taken forward if there is a will to seek the extraterritorial enforcement of DRNs, and at least some prospect of doing so effectively. It might also be justified on the basis that the mere presence of the power on the statute book will be of assistance in securing the cooperation of foreign TOs, whether because they are intimidated by it or because they will find it easier to cooperate freely if they can cite to directors or shareholders the risk of enforcement action if they do not.

5.29. I was informed that no policy position has yet been taken within government as to whether to advance these proposals or to proceed on another basis: for example, by issuing enforceable TCNs in relation to interception, or by securing compliance with DRNs without the need for enforcement action. In the circumstances, while generally accepting of provisions for extraterritorial

153 AQOT §14.59.

enforcement on the pragmatic basis advanced in AQOT, I make no recommendation on this issue.

6. CHANGES TO DEFINITIONS

The definitions in issue

6.1. The Home Office Report stated that *'the primary objective of reviewing the definitions within the Act was to ensure that the way specific terms are defined remains fit for purpose in enabling public authorities to fulfil their statutory functions'*.[154] Three definitional issues in particular were identified. The first two relate to the circumstances in which public authorities can lawfully acquire CD from TOs. They are, in summary:

- ***The definition of CD in IPA s261***. A public authority must obtain authorisation under Part 3 of the Act before obtaining CD from a TO. However, recent technological developments mean that it is not always clear whether a particular type of data falls within the scope of the definition of CD. The ambiguity in the definition has created confusion amongst public authorities as to when it is necessary to obtain a Part 3 authorisation or where a separate notice is required under the DPA 2018.

- ***The lack of definition of 'lawful authority' for the purposes of s11(3).*** S11(1) imposes criminal liability on an individual from a public authority which *'knowingly or recklessly obtains communications data from a telecommunications operator or a postal operator'.* Whilst s11(3) provides that no offence is committed where the person *'acted in the reasonable belief that the person had lawful authority to obtain the communications data'*, there is no statutory definition of what is meant by lawful authority for the purposes of this section. This has created uncertainty as to the circumstances in which public officials can lawfully acquire CD.

6.2. The third area concerns the definition of ***interception of communications*** and the ambit of the offence of unlawful interception under IPA s3.

6.3. Accordingly, my Terms of Reference asked me to consider whether changes to certain definitions within the Act *'are required and whether these would be practicable and desirable'*.

[154] Home Office Report, p11.

6.4. I summarise the consultation responses before addressing these definitional issues in turn.

6.5. Both Graham Smith and Professor Peter Sommer commented on the practical difficulties in applying the existing definition of CD. Professor Sommer referred specifically to the difficulties in separating CD from content (further addressed below), particularly in the context of ICRs.[155] A similar point was made by Graham Smith. In his view, the Home Office should provide a comprehensive list of datatypes, setting out whether or not each falls into the category of CD and the reasons why that is the case.[156]

6.6. Both also agreed that the current definition of interception posed interpretative challenges. Professor Sommer pointed out that *'concepts of "interception" have had to become more complex as technology developed'*.[157]

Definition Issue 1: Communications Data

The Issue

6.7. The IPA was intentionally drafted in a technology-neutral manner, to enable it to accommodate changes in technology without the need for frequent amendment. Though wholly understandable, this approach has led to a degree of ambiguity in the way certain definitions within the Act are applied to different types of technology.[158] The definition of CD in IPA s261 is an example of this. In the words of the IPC's 2021 Annual Report:

> 'An area that caused significant challenge for OCDA throughout 2020 and 2021 is what has become colloquially known as the IPA versus DPA (Data Protection Act 2018) issue. This was reported in detail in our last two reports. The Investigatory Powers Act 2016 (IPA) brought changes to the definitions of communications data (CD) and telecommunications operators (TO). It also prohibited (via the Code of Practice) the use of data protection legislation to circumvent requesting CD under the IPA and introduced a criminal offence of knowingly or recklessly obtaining CD from a TO without lawful authority. This has resulted in public authorities seeking IPA authorisation to acquire information that would previously have been acquired using data protection provisions. In turn, this has presented difficulty for OCDA in that it can only grant authorisation to acquire data that falls within the complex and ambiguous definition of CD under the IPA. At times, this has led to conflict with some public authorities faced with a TO refusing to disclose CD otherwise than by

155 Professor Peter Sommer response, §10. Graham Smith response, §§50-51.

156 Graham Smith response, §27.

157 Professor Peter Sommer response, §27.

158 This point was forcefully made by Graham Smith in his consultation response. He stated that *'for all the desire that the IP Act should be more readily comprehensible than RIPA, it was evident from the outset that partly in order to achieve future-proofing the data definitions, in particular, were drafted at a level of abstraction that presented a systematic obstacle to comprehension'* (§38).

response to an IPA authorisation, and OCDA declining to grant such an authorisation where the information being sought could not clearly be defined as CD.'[159]

6.8. CTP emphasised the practical difficulties that LE encounter in determining whether data falls within the definition of CD, and IPCO pointed me to two aspects of the definition of CD that are particularly difficult to apply in practice. This led the Home Office to issue additional guidance in November 2021 to the operational community, agreed with both IPCO and OCDA, which addresses both the scope of CD and the definition of a TO. That guidance was published, after a time lapse which I am told was intended to allow operational partners to undertake the necessary changes, in April 2023.[160]

6.9. First, it can be difficult to establish whether data either *'relates to the provision of a [telecommunications] service'* (s261(5)(a)(i)) or *'relates to the use of a telecommunications service of a telecommunication system'* (s261(5)(a)(iii)), so as to fall within the definition of CD (assuming it is not content).[161] This is especially the case where the business does not operate exclusively as a TO. In those cases, the public authority must consider what data the business holds as a TO and what data it holds for other purposes. This can be a tricky distinction to make. Take the example of an online video streaming business. The Home Office guidance states that payment details provided to stream a particular video within a limited time is CD because the payment is made in exchange for the provision of a communication service (here, the right to stream the video). However, payment details provided to download a particular video permanently are not deemed, under the guidance, to be CD. This is because the payment is in exchange for '*purchasing*' the file, rather than provision of a telecommunications service.

6.10. Second, IPA s261(5) expressly carves out *'any content of a communication*' from the definition of CD. Content of a communication is defined in s261(6). But establishing whether data is content is not straightforward, particularly in relation to what is often called '*subscriber data*' or '*account data*'.[162] For example, an individual's name may be included in an electronic form when opening an online account. On clicking '*submit*', the form is sent to that company's servers. The online form is CD but it includes 'content' in respect of information entered on

159 Annual Report of the Investigatory Powers Commissioner 2021, March 2023, §2.9.

160 Home Office, *Additional Guidance to the communications data code of practice: definition of communications data*, April 2023.

161 I am told that determination of whether data falls within s261(5)(a)(ii) of the Act is more straightforward in practice.

162 Subscriber or account data *prima facie* falls within the definition of CD as it is entity data under IPA s261(3)(b), namely *'data which identifies or describes the entity'*. The terms subscriber data (which I use in this Report) and account data appear to be used interchangeably.

the form, such as the individual's name. In many cases, whether data amounts to content may depend upon the way the TO originally obtained the data. This itself poses problems because:

- The way in which the TO obtained the data will not necessarily be obvious to the public authority at the time they wish to obtain that data.

- A TO may not store and categorise information on the basis of how it was originally obtained. A consequence of this is that when a TO is issued with a notice to disclose CD, it can be difficult for that operator to separate out content data (which falls outside the scope of the notice) from other subscriber data it holds.

Discussion

6.11. I agree with the IPC that there is a strong case for legislative clarification.[163] As the IPC remarked in his 2021 annual report:

> '[B]oth operational professionals and the public should be able to understand with relative ease what data is CD and what data is not. It cannot be right that only a combination of systems engineers and legal experts poring over the legislation and Code of Practice can reach a tentative conclusion on what is the most widely used investigative power'.[164]

6.12. The Home Office's proposal is that s261 is amended to make clear that there is no carve-out for content in respect of subscriber data.[165] This proposal would eliminate some of the current uncertainty. Having determined that the data relates to either the provision of a telecommunications service or the use of a telecommunications system, there would be no need for public authorities to go on to consider whether such data was content. It would fall within the scope of CD, and therefore of IPA Part 3. Such an amendment would be a welcome simplification.

---

163 IPCO Annual Report 2021, March 2023, 2.16.

164 *Ibid.*, 2.11.

165 The equivalent provision of RIPA (the predecessor to the IPA) included subscriber/account data within the definition of CD and did not seek to carve out the content of the communication. CD was defined in RIPA ss21(4)(a)-(c). Under s21(4)(c), the definition of CD included subscriber data: *'any information not falling within [the preceding paragraphs] that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service'.* In contrast with s21(4)(b), there was no carve out for the content of such a communication under s21(4)(c).

6.13. It might however be questioned whether this amendment goes far enough to address all the practical issues with the application of the current definition of CD. Three such issues were drawn to my attention by IPCO:

- It would remain difficult to determine, as a first step, whether data relates to *either* the provision of a telecommunications service *or* the use of a telecommunications system, so as to fall within the definition of CD. This issue is addressed at 6.9 above. That will remain an issue not only in respect of subscriber data but in relation to further types of data such as payment data.

- There are other types of data, in addition to subscriber data, which are difficult in practice to classify as content on the one hand or CD on the other. One such example given by IPCO is location data, with the view being taken in the guidance that a phone's cell site data is CD but data which indicates the actual location derived from the '*location service*' within a device is not CD. Thought should be given to whether any other types of data should also be expressly excluded from the carve out for content.

- There is at least a question mark over whether it remains necessary to distinguish between '*entity data*' and '*events data*' within s261 of the Act. I understand from IPCO that considerable time and resources are currently spent determining into which of these two categories data properly falls. Entity data is currently subject to a lower threshold for authorisation[166] as it was originally thought to cause less intrusion into privacy. It is for consideration whether this remains the case.

6.14. ***I recommend that the definition of communications data in IPA s261(5) is amended so that the carve-out for content does not apply in respect to subscriber data. Other related clarifications should be considered.***

Definition Issue 2: Lawful Authority

The issue

6.15. Under IPA s11(1), it is a criminal offence for an individual from a public authority to *'knowingly or recklessly obtain[] communications data from a*

[166] Under s60A(8)(a), events data can only be obtained in the context of crime where it is for the purpose of *'preventing or detecting serious crime'*. There is no requirement of seriousness in respect of the obtaining of entity data; under s60A(8)(b), entity data can be obtained for *'the purpose of preventing or detecting crime or of preventing disorder'*.

telecommunications operator or a postal operator'. IPA s11(3) provides a defence to criminal liability where *'the person acted in the reasonable belief that the person had lawful authority to obtain the communications data'*. There is currently no statutory definition of what is meant by lawful authority for the purposes of s11(3). This is in contrast to *'lawful authority to carry out an interception'*, which is precisely defined in IPA s6.

6.16. The lack of clarity concerning the circumstances in which an officer can lawfully obtain CD compounds the uncertainty caused by the ambiguity in the definition of CD. I am told this can discourage officers from seeking CD because of concerns that they may inadvertently commit a criminal offence.[167]

Discussion

6.17. The Home Office proposal is to introduce a statutory definition of *'lawful authority*' for the purposes of IPA s11. This would provide greater certainty to public officials considering obtaining CD from TOs. Whilst the terms of any amendment are for others to decide, it would appear sensible if the definition broadly mirrored the definition of *'lawful authority'* for the purposes of interception in IPA s6.[168]

6.18. The statutory definition should also encompass the following two situations in which lawful authority to obtain CD is currently recognised by the CD Code of Practice. Those are:

- ***Specific matters in the public interest***: Chapter 10 of the CD Code of Practice sets out special rules on the granting of authorisations and giving of notices in specific matters of public interest. In respect of 999/112 calls, the code recognises an '*emergency period of one hour after the termination of the emergency call in which disclosure of communications data to emergency services will largely fall outside the provisions of the Act*'.

- ***Publicly or commercially available data***: The CD Code §15.11 states that it is not necessary to seek authorisation to obtain CD where that

[167] A person is excluded from criminal liability where they act in the reasonable belief that they had lawful authority to obtain the CD. This provides some protection to officers, but does not diminish the need for 'lawful authority' to be given statutory definition within the Act.

[168] This would cover CD obtained in accordance with (a) an authorisation made under IPA Part 3, (b) a bulk / targeted interference warrant, (c) a bulk/ targeted equipment interference warrant, (d) the exercise of a statutory power exercised for the purpose of obtaining information or taking possession of any document or other property, *or* (e) a court order.

data *'is made publicly or commercially available by the telecommunications operator or postal operator'.*

6.19. A more nuanced issue is whether the statutory definition of lawful authority should also encompass the situation, set out in the CD Code §15.11, in which *'the telecommunications operator or postal operator freely consents to its disclosure'*. On the one hand, it is arguable that no Part 3 authorisation should be required when data is voluntarily provided by the TO. On the other hand, the same intrusion into privacy occurs regardless of whether the operator provides data voluntarily or is compelled to do so; and it is possible that issues could arise as to whether consent was freely given.[169] This issue is currently the subject of detailed discussions between IPCO and the government. In the circumstances, I make no specific recommendation.

6.20. Overall, it is desirable that the situations in which an individual avoids criminal liability are not simply set out in the Code of Practice but receive statutory underpinning. ***I recommend that a statutory definition of lawful authority to obtain CD is introduced, to include certain situations where lawful authority is currently recognised by the CD Code of Practice.***

Definition Issue 3: Interception

6.21. Under IPA s3, a person commits the offence of unlawful interception where (a) the person intentionally intercepts a communication in the course of its transmission[170], (b) the interception is carried out in the UK and (c) the person does not have lawful authority to carry out the interception. A detailed definition of interception is contained in IPA s4. This addresses what it means both to intercept a communication in the course of its transmission (ss4(1)-(7)) and to carry out interception in the UK (s4(8)). IPA s6 provides a definition of lawful authority to carry out interception.

6.22. Much of the language used in IPA ss3 and 4 is based on that used in RIPA ss1 and 2. When RIPA was first enacted, more than 20 years ago, telecommunication systems were simpler. They were less fluid and less interconnected. However, the rapid pace of technological change, and development of cloud capabilities in particular, has led to increasingly complex data flows. This poses challenges to the

169 Though any such risk could be mitigated: CD Code §15.11, echoing §1.5, also provides that public authorities should not require, or invite, TOs to disclose CD by relying on statutory exemptions to restrictions on disclosing personal data.

170 Under IPA s3(1)(a), the communication must be in the course of its transmission by means of (i) a public telecommunication system, (ii) a private telecommunication system or (iii) a public postal service.

practical application, and continued efficacy, of the current definitions. I see the benefit of potential amendment to the current provisions.

6.23. However, the Home Office did not provide me with a firm proposal on this issue and I understand that the need for legislative change is not considered urgent. It became apparent during the course of my Review that amendment of these complex provisions would have wide-ranging ramifications, requiring detailed consideration and consultation with stakeholders to a longer time-frame.[171] Accordingly, by agreement with the Home Office, I make no specific recommendation in relation to this issue.

[171] An idea of the multiple '*interpretative challenges*' in this area can be gleaned from Graham Smith's *Internet Law and Practice* (Sweet & Maxwell, 5th edn. 2019), §8-037 - §8-121, referred to in his response to the Review at §51.

7. TARGETED EXAMINATION WARRANTS

Existing system

7.1. Bulk interception and EI warrants, available only to UKIC under IPA Part 6, must have as their main purpose the obtaining of overseas-related communications, information or data.[172] But even overseas-related communications may involve persons in the UK; and these bulk powers will inevitably capture some material which is not overseas-related at all. The safeguards applied by the IPA to the selection for examination of material collected under a bulk warrant thus include a prohibition on using criteria for examination whose purpose is to identify material that is sent by, or intended for, an individual known to be in the British Islands.[173]

7.2. Where an intelligence agency does wish to select for examination material obtained from bulk interception or bulk equipment interference that is sent by, or intended for, someone in the British Islands, it must obtain a targeted examination warrant (**TEW**).[174] The purpose of a TEW is to give additional protection, not to British citizens (for the IPA does not distinguish by citizenship) but to persons within the British Islands. Given that material acquired under bulk powers should be overseas-related, it is thought likely to contain less information relating to individuals located in the British Islands than would be provided by techniques authorised by, for example, a targeted interception warrant.

7.3. TEWs may be specific to a particular person, organisation or set of premises. Alternatively, like other types of targeted warrants, they may be thematic in nature.[175] Thematic warrants may relate to:

- *'A group of persons who share a common purpose or who carry on, or may carry on a particular activity';*[176]
- *'More than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation'*; [177] or

---

172 IPA s136 (bulk interception); s176 (bulk EI). 'Overseas-related' means, in essence, either sent or received by individuals who are outside the British Islands (i.e. the UK, Channel Islands and Isle of Man).

173 IPA s152(4) (bulk interception); s193(4) (bulk EI).

174 TEWs relating to bulk interception are provided for under IPA ss15(1) and (3). TEWs relating to bulk EI are set out in IPA ss99(1) and (9).

175 IPA ss17(2), 101(2).

176 IPA ss17(2)(a), 101(2)(b).

177 IPA ss17(2)(b), 101(2)(c).

- Testing or training activities.[178]

7.4. It is the first category of thematic warrant that is most commonly used in target discovery. In practical terms, there are two distinct stages to the application for, and execution of, such a warrant:

- An Agency sets out a description of the warrant's subject matter on the face of the warrant (**Stage 1**). Where the warrant relates to a group of persons who share a common purpose or who carry on, or may carry on, a particular activity, then the warrant must provide a description of that purpose or activity. This could be, for example, individuals carrying out a particular crime.

- An Agency devises search criteria that should result in the selection of only that material that relates to those individuals falling within the described *'group of persons'* (**Stage 2**).

TEW Issue: Incidental Conduct Power

7.5. Difficulties have been identified in devising search criteria which eliminate any possibility that at least some material selected will concern individuals not falling within the '*group of persons*' described on the warrant (i.e. false positives). By way of hypothetical example, a thematic TEW could authorise the discovery of previously unidentified terrorists by looking for a suspicious combination of observable actions (for example, accessing particular online sites). The search criteria might highlight a small number of individuals who perform all those actions but who do not subsequently meet the investigative priority threshold, for example because they are *bona fide* researchers. There is a risk of unauthorised selection for examination in relation to individuals later found to fall outside the scope of the thematic TEW.

7.6. The Home Office's proposal is that an '*incidental conduct*' power be introduced in respect of TEWs. This would authorise not only the conduct described in the warrant but '*any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant*'. In that way, it would replicate the incidental powers that currently attach to two other types of targeted warrant: targeted interception warrants (IPA s15(5)) and targeted EI warrants (IPA s 99(5)). The Home Office suggests that this would provide a statutory safety net

[178] IPA ss17(2)(c), 101(2)(d)-(e).

for those instances where the results of Stage 2 do not align perfectly with the description of *'the group of persons'* in Stage 1.

7.7. Nothing was said about TEWs in the Home Office Report or in my Terms of Reference. The List of Specific Topics did however ask whether IPA ss15(5) and 99(5) should also apply to TEWs. The consultation responses received did not address this issue.

Discussion

7.8. Whenever an Agency uses TEWs for target discovery purposes, it is impossible entirely to eliminate the risk that some of the material selected for examination may relate to individuals who are not of intelligence interest. The key question is how the legislation can best provide both (a) for sufficient safeguards to ensure that collateral intrusion is kept to the absolute minimum and (b) for the intelligence services' conduct to be lawful when unavoidable collateral intrusion does take place.

7.9. The Review team has discussed the Home Office proposal with IPCO. IPCO is keen to explore further with UKIC whether legislative change is absolutely necessary to resolve the operational issue identified above. Whilst further detailed discussion is required, IPCO's initial view is that it may be possible to resolve the operational issue without introducing an '*incidental conduct*' provision. In broad terms, that would be through tweaking the way in which the intelligence services describe the subject matter of the warrant. Much of the detail of discussions on this issue is classified but I make three high-level points.

7.10. ***First***, the narrower the description of the *'group of persons'* at Stage 1, the harder it is to devise Stage 2 criteria that do not risk the selection of material relating to people falling outside that group. Using the example above, if the TEW related to all members of a terrorist group behaving in a particular way, then it may be difficult to devise search criteria that do not also capture persons who behave in that way for non-criminal reasons. That issue would not arise if the warrant was drafted more broadly to capture all individuals displaying the relevant behaviours, regardless of whether they held a criminal intent.

7.11. ***Secondly***, the way in which the subject matter is described on the warrant does not ultimately affect how many people have their communications selected for examination who are not of intelligence interest to the intelligence services. If the warrant is narrowly construed, then the search criteria will inevitably return false positives. If the warrant is more broadly construed, this will eliminate false

positives but result in greater numbers of persons falling within the scope of the warrant who are not actually of intelligence interest to the intelligence services.

7.12. ***Thirdly***, it may therefore be that the operational issue identified could be resolved not through legislative change but by more broadly defining the '*group of persons*' at Stage 1. It may be that this could be achieved by focusing more on the activity of the group in question, rather than the persons undertaking that activity. This would shift the focus to the activity of the individuals and away from individuals' underlying motive in carrying out those acts.

7.13. In light of the fact that discussions are still ongoing, and that IPCO has taken no clear position in favour or against the Home Office proposal, I decline to make a recommendation on this issue.

8. WARRANTRY PROCESS

Existing system

8.1. The central feature of the IPA's safeguard regime is the 'double lock': the requirement that various types of warrants be issued by the Secretary of State and approved by JCs.[179] For warrants relating to communications sent by, or intended for a member of a relevant legislature, a 'triple lock' applies: the Secretary of State may not issue a warrant without the additional approval of the Prime Minister.[180]

Terms of reference and consultation

8.2. The Home Office Report did not question the principle of the double or triple lock, and did not recommend major changes to its application. It did however identify what it described as '*pressure points in the warrantry process which may ultimately require legislative change*'. The impetus towards greater resilience derived in part from the unavailability through illness of key decision-makers (e.g. the Prime Minister in April 2020 and the Director General of the NCA from July to October 2021).

8.3. My Terms of Reference (pp 8-9) accordingly asked me to consider

> '*improvements to the warrantry process to increase efficiency and strengthen resilience whilst maintaining appropriate safeguards*'.

8.4. The List of Specific Topics elaborated the proposed improvements in the following terms:

- Consider the need to provide resilience in the approval process for Targeted EI warrants, as the Director General NCA is the only law enforcement chief within the NCA who is able to authorise these warrants: s106 and Schedule 6

- Consider the need to provide resilience in the approval process for ss26/111 triple locked warrants where the Prime Minister is unavailable or incapacitated

---

179 Targeted interception warrants, TEWs and mutual assistance warrants (Part 2 chapter 1); targeted EI warrants and TEWs (Part 5); bulk interception warrants, bulk acquisition warrants and bulk EI warrants (Part 6); BPD warrants (Part 7). Other powers, thought to be less intrusive, are subject to different mechanisms for authorisation.

180 IPA ss26, 111.

- Consider whether the process for obtaining the assistance of a TO in EI operations is efficient (ss126/128).

8.5. A further proposal put to me by the Home Office was that s121 should be amended to remove the obligation for the Secretary of State to be notified personally when a senior official modifies a targeted EI warrant to remove matters, names or descriptions.

Warrantry Issue 1: NCA Authorisation of TEI warrants

8.6. IPA s106 empowers '*law enforcement chiefs*' listed in Schedule 6 to issue a targeted EI warrant under specified conditions. The first column of Tables 1 and 2 in Schedule 6 list a number of LE chiefs, including the Metropolitan Police Commissioner, Chief Constables and the Director General of the NCA.

8.7. IPA s106(4) allows '*an appropriate delegate*' to exercise the power '*in an urgent case*'. Appropriate delegates for each category of LE chief are listed in the second column of the Schedule 6 Tables: the appropriate delegate in the case of the NCA is a senior NCA officer designated for the purpose by the Director General.

8.8. When the Director General of the NCA was unavailable through illness for a period in 2021, IPCO pragmatically agreed to treat the situation as one of urgency and to allow targeted EI warrants to be issued by a designated senior NCA officer.[181] Operational effectiveness was therefore maintained, though the definition of '*urgency*' was arguably stretched in the process. For that reason and in order to allow the spreading of the workload that would otherwise be placed on the Director General (over 100 new targeted EI warrants were issued in 2021), the solution recommended by the Home Office is to consider amending the IPA to allow senior NCA officers other than the Director General to authorise targeted EI warrants.[182]

8.9. It is plainly sensible for such a solution to be put into law, either uniquely for the IPA (by amendment of Schedule 6) or more generally by amendment of s41 of the Police Reform and Social Responsibility Act 2011. There being no statutory post

[181] Warrants remained subject to the double lock.

[182] The problem is unique to the NCA, notwithstanding that other law enforcement chiefs are listed in the first column of the Schedule 6 tables, because s41 of the Police Reform and Social Responsibility Act 2011 allows deputy chief constables to exercise or perform any of the functions of chief constables when they are unable to do so. That section has no application to the NCA.

of Deputy Director General of the NCA, it may be necessary to specify any person holding Director General rank within the NCA.[183]

8.10. ***I recommend that provision be made in law for senior officers of the NCA other than the Director General to authorise targeted equipment interference warrants.***

Warrantry Issue 2: Securing the Triple Lock

8.11. Few investigatory powers issues are more sensitive, at least to parliamentarians, than the question of whether and if so on what conditions UKIC and LE may obtain and read the communications of MPs, peers and other legislators.

8.12. The Investigatory Powers Tribunal (**IPT**) ruled in 2015 that the so-called Wilson Doctrine affords neither a legal guarantee nor a substantive legitimate expectation to MPs that their communications will not be intercepted.[184] The legislative response was IPA ss26 and 111, which apply where:

- the purpose of a targeted interception warrant is to authorise or require the interception of communications sent by, or intended for, a member of a relevant legislature;[185]
- the purpose of a TEW is to authorise the selection for examination of the content of such communications;[186]
- the purpose of a targeted EI warrant is to obtain communications sent by, or intended for, a member of a relevant legislature, or a member of a relevant legislature's private information;[187] and where
- the purpose of a TEW is to authorise the selection for examination of protected material which consists of such communications or private information.[188]

In each case, the usual double lock is supplemented by an unqualified requirement that the Secretary of State may not issue the warrant without the

183 The current leadership structure comprises three persons with Director General rank serving under the Director General of the NCA.

184 *Caroline Lucas and others v Security Service and others* [2015] UKIPTrib 14_79-CH. The Wilson Doctrine is explained in this House of Commons library note of 2017.

185 IPA s26(1)(b)(i). Relevant legislatures are the House of Commons, House of Lords, Scottish Parliament, National Assembly for Wales and Northern Ireland Assembly.

186 IPA s26(1)(b)(ii).

187 IPA s111(1).

188 IPA s111(2).

approval of the Prime Minister. Use of the triple-locked powers is not confined to circumstances where a legislator is the person under investigation: the triple lock applies equally where a subject of interest has been communicating with a legislator.

8.13. The hospitalisation of the then Prime Minister in April 2020 rendered the triple lock unavailable, and prompted consideration of whether a power to appoint an alternate or deputy was needed. There are precedents for such procedures in relation to other critical national security authorisations which require Prime Ministerial approval.

8.14. It seems obvious that such a procedure is called for. The issues are (1) who should be authorised to deputise for the Prime Minister, and (2) in what circumstances.

8.15. As to issue (1), the baseline requirement is that a Secretary of State should be available to deputise for the Prime Minister, other than the Secretary of State who authorised and will issue the warrant. Since any holder of the office of Secretary of State is eligible to authorise a warrant, at least two alternate deputies will be required if a triple lock is to be feasible in all cases.

8.16. The option suggested to me by the Home Office would require successive Prime Ministers to designate a list of alternates, with or without specifying a hierarchy. The longer that list, the more flexibility in the system but the greater the risk that the final component of the triple lock would be applied by a person unfamiliar with warrantry requirements. The list would have to be amended when a designated person left the Cabinet.

8.17. Whether this or some more prescriptive system is adopted, there would in my view be sense in designating as deputies (whether by law or as a matter of practice) the Home Secretary and Foreign Secretary, together with the Secretaries of State for Northern Ireland and/or Defence if more flexibility is thought desirable.[189] The holders of those posts enjoy secure arrangements for dealing with warrants and (unless very new in office) will have experience in warrantry. The number of people aware of sensitive warrant information would thus be kept to a minimum.

8.18. As to issue (2), one (narrow) option would be to allow the use of a deputy only when the Prime Minister is incapacitated. A second option would be to allow the

[189] Since the Home Secretary or Foreign Secretary authorise most of the warrants, to name only them as triple-lock alternates might result in delay if one had authorised a warrant and the other were, for example, travelling abroad. The Deputy Prime Minister might seem to be a logical alternate, but the post is not recognised in law, and is not always filled.

use of a deputy also when the Prime Minister has a conflict of interest, or is unable to communicate securely, e.g. because of foreign travel. A third, less specific option would be to allow the use of a deputy where the Prime Minister is unable to exercise the function for any reason.[190] While that option would be usefully flexible, the extreme sensitivity of the subject-matter might favour something more constraining of the use of deputies. I make no recommendation as between the second and third of these options.

8.19. To limit the deployment of a deputy to '*urgent*' cases might be unwise, since it would require routine warrants to be classified as urgent in the event of a lengthy period of incapacity, replicating the problem encountered under s106(4) (Warrantry Issue 1: 8.8 above). The problem might be surmounted, in this case as in that one, by recourse to the concept of the required timescale.

8.20. ***I recommend the use of a deputy to be permitted for the purposes of the triple lock when the Prime Minister is unable to approve a warrant to the required timescale (in particular through incapacity, conflict of interest or inability to communicate securely).***

Warrantry Issue 3: Notification on Modification of Targeted EI Warrant

8.21. This issue raises a simple point of principle: whether the Secretary of State should have to be notified when the scope of a targeted EI warrant is reduced. It arises in the following statutory context:

- IPA s118 makes provision for targeted EI warrants issued by the Secretary of State, Chief of Defence Intelligence or Scottish Ministers to be modified by them.
- IPA s119(1) permits such modifications to be made also by a senior official acting on behalf of the Secretary of State or Scottish Ministers.
- IPA s120 makes a distinction between:
    - modifications '*removing any matter, name or description*' from a warrant, in respect of which (unsurprisingly) no conditions apply, and

[190] Cf. IPA s227(9A), which permits the IPC to delegate certain functions when 'unable to exercise the functions because of illness or absence or for any other reason'; see also s41 of the Police Reform and Social Responsibility Act 2011 (above).

- other modifications (e.g. adding a name, description or type of equipment included in the warrant) which must be necessary and proportionate and respect where applicable the additional safeguards in ss111-114.

- IPA s121 imposes notification requirements when modifications are made by (a) the Secretary of State or Scottish Ministers (s121(1)) and (b) senior officials (s121(3)). In the former case, a JC must be notified; in the latter case, the Secretary of State or a member of the Scottish government '*must be notified personally of the modification and the reasons for making it*'.

- IPA s121(2) waives the notification requirement under s121(1) when the modification is '*to remove any matter, name or description*' included in the warrant in accordance with ss115(3) to (5). This picks up the s120 distinction noted above, though in a different context.[191]

8.22. The anomaly identified by the Home Office is the absence of any waiver, equivalent to s121(2), of the s121(3) notification requirement.

8.23. I agree that there is no obvious reason why the Secretary of State should need to be notified of the *removal* of a name, matter or description from a warrant. The effect of such removals is to end or reduce an existing course of EI: they neither enable new EI to take place nor intrude further into individual privacy. A waiver would reduce the administrative burden attached to the process, remove the anomaly identified above, and release capacity for more important matters.

8.24. ***I recommend that IPA s121 be amended so as to provide that s121(3) does not apply when the modification is to remove any matter, name or description included in the warrant in accordance with ss115(3)-(5).***

Warrantry Issue 4: Obtaining the Assistance of TOs in EI Operations

8.25. Some targeted EI techniques under Part 5 of the IPA require the assistance of a TO.

8.26. As noted under Warrantry Issue 1 above, LE chiefs may issue targeted EI warrants under IPA s106. IPA s126 permits '*implementing authorities*' to request the assistance of other persons, including TOs, in giving effect to targeted EI warrants. This procedure is adequate when a TO is willing to assist voluntarily. Sometimes,

[191] There are further waivers of the notification requirement, not relevant here, when the modification was made by other persons pursuant to urgency provisions, and when the additional safeguards in ss111-114 apply.

however, TOs require compulsion to support EI operations; and s126 contains no power of compulsion. The Review team was shown operational examples of two time-sensitive murder investigations in which potentially fruitful lines of enquiry were frustrated for lack of a power to compel TOs to assist the police with their enquiries.

8.27. IPA s128 does contain a power by which TOs can be compelled to take all steps that are notified to them for giving effect to a targeted EI warrant. That power however exists only in relation to warrants issued by the Secretary of State, the Chief of Defence Intelligence or the Scottish Ministers. It does not exist in relation to warrants issued by LE chiefs under s106. The only option open to a LE authority wishing to resort to compulsion is thus to apply (through one of the intermediaries listed in s128(3), generally the NCA) for a warrant authorised by the Home Secretary and then approved by a JC.

8.28. The Home Office told the Review team that there may be scope for avoiding a new power of compulsion via training for police and consultation and negotiation with TOs. Others suggested that it might be possible to solve or at least mitigate the problem by streamlining the process for LE chiefs to invoke s128. This could be done by removing the s128(3) requirement on most forces to use the NCA or another intermediary to approach the Secretary of State.

8.29. There is a strong public interest in ensuring that TOs give effect promptly to targeted EI warrants issued by LE chiefs under s106. Since the Home Office has not reached a concluded view as to whether legislation is necessary, I make no formal recommendation on this issue. However, having spoken to IPCO I understand that the requirement of Secretary of State authorisation under IPA s128 has value, while the s128(3) requirement that an intermediary be used may not. On that basis, if it is decided to seek change to the legislation, the options to be considered should include the amendment of s128 so as to remove the requirement that most LE chiefs approach the Secretary of State via an intermediary.

9. OVERSIGHT

Existing system

9.1. The use of covert investigatory powers under the Act is subject to the oversight of the IPC and 17 JCs, each of whom must be a serving or former senior Judge.[192] Approval from the IPC or a JC is normally required before certain categories of warrant may enter into force.

9.2. The main oversight functions of the IPC are set out in IPA s229 (main oversight functions) and s230 (additional directed oversight functions).

9.3. The IPC is supported by IPCO, an office with a Chief Executive and around 50 employees who include inspectors with expertise in the capabilities for which the Act provides.[193] The IPC also has responsibility for OCDA, which provides for the independent authorisation of most CD requests. The TAP, set up on the recommendation of the RBPR, advises the IPC on the impact of changing technology and its impact on privacy.[194]

9.4. The IPC may decide to delegate functions to a JC.[195] That power does not however extend to matters relating to the appointment of JCs and TAP members, or (save where the IPC is unable to exercise the functions because of illness or absence or for any other reason) to the IPC's functions relating to CD under ss60A and 65(3B).[196]

Terms of Reference

9.5. The government's review of the IPA found no case for systemic change to the IPC's role or current legal basis. The Home Office Report did however note that the Covid-19 pandemic had highlighted the need for resilience and flexibility to be embedded within the Act, and recorded that several pragmatic proposals had been identified and approved by IPCO. Reference was made in this connection to delegation of the IPC's functions, including the appellate function and functions related to CD, and to the creation of a statutory basis for the appointment of

192 IPA s227. The first two Investigatory Powers Commissioners were Rt. Hon. Sir Adrian Fulford, then a serving Lord Justice of Appeal, and Rt. Hon. Sir Brian Leveson, a former Lord Justice of Appeal.

193 They have expertise also in other capabilities for which IPCO is responsible under Acts other than the IPA, such as the handling of covert human intelligence sources and directed and intrusive surveillance.

194 IPA s246.

195 IPA s227(8).

196 IPA ss227(9) and (9A).

Deputy IPCs. Both the Terms of Reference and the List of Specific Topics alluded to these matters without giving further detail.

Consultation

9.6. Some (but not all) of the Oversight Issues identified below were specifically flagged in the Home Office Report, Terms of Reference and List of Specific Topics. Those that were flagged attracted little interest and no objections from those who responded to the consultation.

9.7. Liberty and Privacy International however raised a number of broader points regarding the oversight process, which they consider to be inadequate and in need of improvement.

9.8. Proposals advanced by Privacy International included:

- empowering IPCO to assess for itself whether a warrant is necessary and proportionate, rather than applying the judicial review test to the conclusions of the Secretary of State;
- institutional separation of the warrant authorisation and oversight functions;
- ensuring that IPCO is fully resourced to conduct audits and reviews over each Agency; and
- empowering oversight bodies to undertake meaningful human rights assessments prior to the deployment of new systems and technologies.[197]

9.9. Liberty called for:

- stronger statutory duties on state bodies exercising IPA surveillance powers to disclose all relevant information during the warrantry process, and more generally to oversight bodies;
- stronger statutory duties and powers to audit on the part of IPCO and the Home Office, generally and to ensure that the conditions for warrantry have been made out; and

[197] Privacy International, consultation response §§4.45, 6.3.

- statutory duties imposed on state bodies exercising IPA surveillance powers to report to the public systemic non-compliance with statutory safeguards in relation to bulk surveillance.[198]

In support of the latter point, Liberty recalled that the factual details underlying the *TechEn* case (Annex 4 to this Report, §§5-9) came to light only when the government was required to produce them pursuant to its duty of candour to the court.

9.10. It is unquestionably correct that IPCO (and any other relevant oversight body) should be sufficiently resourced, and that it should undertake human rights assessments prior to approving the deployment of new systems and technologies. The other issues raised, most of which were the subject of extensive debate during the passage of the IPA, fall outside my Terms of Reference.

Oversight Issue 1: Appointment of Deputy IPCs

9.11. There is no basis in the IPA for the creation of deputy IPCs, drawn from the ranks of the JCs, to whom the functions reserved to the IPC could be delegated in appropriate circumstances.[199] This omission places the agility and resilience of IPCO at risk, particularly during an emergency or when the IPC (who is contracted to work three days per week) is otherwise unable to discharge the functions unique to the IPC.

9.12. The Home Office suggests that two deputy IPCs be appointed, given that JCs are contracted to work for 90 days per year and there is therefore always a risk that a single deputy would be unavailable. IPCO has concurred with this proposal.

9.13. The full mechanism for the appointment of the IPC and JCs would not need to be invoked for the appointment of a deputy, given that any deputy IPC would already have undergone the JC appointments process. It is accordingly proposed that the re-appointment and removal from office of deputy IPCs should be the sole responsibility of the IPC. I agree.

9.14. ***I recommend that statutory provision should be made for the IPC to nominate two deputy IPCs to whom functions currently reserved to the IPC may be delegated.***

198 Liberty, consultation response §18.

199 These functions are summarised under Issue 2, below.

Oversight Issue 2: Delegation of IPC's functions

9.15. A number of important functions under the IPA can currently be discharged only by the IPC. These are, in summary:

(a) the appointment of JCs and members of the TAP[200] (and, if my recommendation on Oversight Issue 1 is followed, the nomination of deputy IPCs).

(b) the determination of '*appeals*' on the part of public authorities whose applications are refused by JCs,[201] and

(c) the grant of authorisations for public authorities to obtain CD.[202]

The case for delegating these functions is addressed by reference to each of them separately.

9.16. As to function (a), these appointments will not generally be so time-sensitive that they cannot wait until the IPC has recovered or is otherwise available. Nonetheless, it would be undesirable if much-needed JCs, TAP members and even deputy IPCs could not be appointed because of the prolonged incapacitation of the IPC. It is also conceivable that some conflict of interest (for example, a family relationship) might make it preferable for an appointment to be made by a deputy IPC. ***I recommend that deputy IPCs should have the power to appoint JCs, members of the TAP and deputy IPCs when the IPC is unable to act within the required timescale.***

9.17. As to function (b), there is a clear operational case for appeals to be dealt with by the new deputy IPCs, in circumstances where they cannot be handled by the IPC. I was told that the issue can arise, in particular, in urgent cases where a JC has ruled that data recovered at the border cannot be retained.[203] Deputy IPCs will be highly respected and capable figures: no particular sensitivity is therefore in play that might require more specific grounds for the delegation than simply inability to act. ***I recommend that appeals should be capable of being determined by deputy IPCs when the IPC is unable to determine them.***

---

200 IPA s247(1).

201 IPA ss23(5), 108(5), 140(4), 146(4), 159(4), 165(4), 179(4), 187(4), 208(4), 216(4); see also Counter-Terrorism and Border Security Act, Schedule 3 paras 13(2), 16(10). The IPA s227(8) power for the IPC to delegate functions to JCs does not appear to apply to this function.

202 IPA s60A.

203 Under Schedule 3 to the Counter-Terrorism and Border Security Act 2019.

9.18. As to function (c), the power of the IPC to grant targeted authorisations for obtaining CD under IPA s60A was added to the IPA in 2018.[204] While the granting of such authorisations is in practice delegated by the IPC to OCDA,[205] I understand that difficulties arose during the pandemic when OCDA (as part of its Business Continuity Plan for highly sensitive CD applications) required JC support and such support was only available from the IPC because, though Covid restrictions made it difficult for him to come into the office, he was arguably not '*unable*' to exercise the functions within the meaning of IPA s227(9A).[206]

9.19. I have no hesitation in accepting that the powers vested in the IPC in relation to authorisations to obtain CD could appropriately be exercised by any JC. They are different in nature to the appointment powers and appeal powers considered under (a) and (b) above. All JCs are hugely experienced and very senior judges, used to making decisions of the highest importance. There are no equivalent limitations on the powers of a High Court, Court of Session or Court of Appeal judge to decide difficult or important cases. The simplest way to effect this change would be to repeal IPA s227(9A).

9.20. ***I recommend that IPA s227(9A) be repealed.***

Oversight Issue 3: Appointment of Temporary JCs

9.21. Temporary JCs, appointed by the IPC under emergency statutory powers,[207] proved vital to the continued operation of the IPA and its oversight regime during the pandemic. Their appointment was required because of the need for JCs to work in a secure environment and because many of them were of an age which rendered them relatively vulnerable to Covid-19.

9.22. The Home Office Review concluded that it would be advantageous to place this power of appointment on a permanent statutory footing, for use in times of emergency so as to maintain the agility and resilience of IPCO and avoid any adverse impact on national security. This strikes me as a sensible precaution.

9.23. Any amendment to the Act would have to specify the range of emergencies in which the power of appointment could be invoked, and to impose limits and

---

204 By the Data Retention and Acquisition Regulations 2018, introduced to give effect to the December 2016 judgment of the CJEU in *Tele 2 and Watson*.

205 IPA s238(5).

206 IPA s227(9A) was added by the Data and Acquisition Retention Regulations 2018/1123, Schedule 1 para 24.

207 Coronavirus Act 2020, s22; The Investigatory Powers (Temporary Judicial Commissioners and Modification of Time Limits) Regulations 2020.

safeguards on that power. The Home Office (without objection from IPCO) proposes that the Covid-19 model is adopted, under which:

- The IPC may appoint temporary JCs to carry out the functions conferred upon JCs. The normal requirements of consultation and joint recommendation[208] would not apply.

- Temporary JCs would be appointed for a period of 6 months (as opposed to the normal 3 years),[209] renewable if necessary. The Home Secretary and the IPC would have to agree that an emergency situation existed before a temporary JC could be appointed or renewed.

- As soon as practicable after the appointment of any temporary JC, the IPC must notify those senior judges and others whose recommendation would normally be required.

9.24. Consistently with the logic of my conclusion under Oversight Issue 2(a) above, ***I recommend that deputy IPCs should have the power to appoint temporary JCs when the IPC is unable to act within the required timescale.***

Oversight Issue 4: Scope for Prime Ministerial Directions

9.25. The IPC has consistently expressed the wish, as noted in the Home Office Report, that its non-statutory functions should be placed on a statutory footing. This wish was recently given effect in relation to the IPC's oversight of:

- GCHQ's Equities Process (the means through which decisions are taken on the handling of vulnerabilities found in technology); and

- LE compliance in relation to the detention and interviewing of detainees overseas and the passing and receipt of intelligence relating to detainees.[210]

9.26. The Prime Minister has a further power under IPA s230 to give a direction to the IPC to keep under review the carrying out of any aspect of the functions of an intelligence service, a head of an intelligence service or any part of Her Majesty's

208 IPA ss227(4)-(6).
209 IPA s228(2).
210 The Investigatory Powers Commissioner (Oversight Functions) Regulations 2022, made under the power in IPA s239 to modify the functions listed in s229.

forces or the Ministry of Defence, so far as engaging in intelligence activities. That power does not however extend to wider public authorities, including LE.

9.27. The Home Office wishes, with IPCO agreement, to fill that gap by extending the functions which may be the subject of a direction to the functions of any public authority, so far as engaging in intelligence activities. This would enable, for example, the NCA and CTP to be included within the scope of a s230 direction with the flexibility that would allow a rapid response to emerging oversight requirements.

9.28. I can see no objection to expanding the category of public authorities whose intelligence-related activities may be the subject of a Prime Ministerial direction to IPCO. On the contrary, such an amendment has the potential to ensure that oversight directions are on a statutory footing, and backed by statutory powers to request information and cooperation. It should also advance transparency by bringing into play s230(4), which requires directions under s230 to be published save in specified circumstances.

9.29. ***I recommend that the list of bodies specified in IPA s230(1) whose intelligence-related activities may be the subject of Prime Ministerial direction to the IPC be expanded to include wider public authorities, so far as engaging in intelligence activities.***

Oversight Issue 5: Oversight of TROs for Prisoners

9.30. Courts have a power to impose telecommunications restriction orders (**TROs**) for the purpose of preventing or restricting the use of mobile telephones &c by persons detained in custodial institutions.[211] This is normally achieved by simply de-activating the prisoner's phone. Use of the power has declined considerably since 2018. The IPC is required to keep its exercise under review.[212]

9.31. The Home Office Review identified that statutory review of TROs for prisoners is of little value. TROs are always authorised by a judge, providing the necessary degree of assurance and oversight. The orders do not contain anything relevant for IPCO to review after the event. It is accordingly proposed, with IPCO's agreement as communicated to me, that this review requirement be repealed. I agree with that proposal.

---

211 Serious Crime Act 2015, s80. s80A was added to the Serious Crime Act in 2017 to provide for drug dealing TROs.

212 IPA s229(3)(c). There is no equivalent requirement of IPC review in relation to drug dealing TROs.

9.32. ***I recommend that IPA s229(3)(c) (review of TROs) be repealed.***

10. THE WAY FORWARD

10.1. The IPA continues to provide a solid and generally satisfactory framework for the regulation of investigatory powers. I believe that it has played a significant part in restoring trust in the UK and abroad after the Edward Snowden revelations of the last decade, and in renewing what has aptly been called UKIC's democratic licence to operate.

The Short Term

10.2. The running repairs recommended in this Report are prompted in part by changes in technology and working methods, but also by simple experience over five years of applying the Act's provisions. They leave its central mechanisms intact, but if enacted in the form I have proposed should give UKIC, LE and indeed IPCO useful extra agility in important areas, without compromising the strong independent scrutiny that is the hallmark of the IPA.

10.3. Police interlocutors raised what they considered to be other pressing legal issues with the Review team, including what they considered to be a legal ambiguity regarding the legal regimes applicable to data stored on the cloud. These matters fell outside the scope of my Terms of Reference but may have to be addressed in another context.

10.4. Once amending legislation is on the statute book, it would be appropriate to start thinking about what comes next.

The Medium Term

10.5. The Home Office Report has already identified two major issues that may need to be addressed in the coming years:

- the bar on using intercept material as evidence in legal proceedings, and the related issue of the distinct legislative treatment of interception and EI;[213] and

[213] IPA s56 (with exceptions set out in Schedule 3); Home Office Report, pp. 17-19; 2.30 above, third bullet. The s56 bar (the successor of a similar bar in RIPA, discussed in AQOT §§9.16-9.18) was supported by some (though not all) of our police interlocutors, who are fearful of the burdensome disclosure requirements that could arise if such evidence were admissible. Professor Peter Sommer put the counter-arguments at §§9-15 and Appendix III to his response to our consultation.

- the challenge posed by the move to end-to-end encryption (where the way forward is said to lie in consensus-building with like-minded governments, rather than legislative change).

10.6. A further group of issues relates to terms that are beginning to look dated, or whose definitions are imprecise. Some examples of the former are identified in the Home Office Report and at 2.30 above. As to the latter, Graham Smith's response to the Review repays detailed study.[214] He makes the important point that legislative change is not always the answer: the publication of interpretations, for example in IPCO advisory notices, serves the interests of transparency and helps avoid what I described in AQOT as obscure laws which '*corrode democracy itself, because neither the public to whom they apply, nor even the legislators who debate and amend them, fully understand what they mean*'.[215]

10.7. More broadly, it is clear that the use of data by police is far from where it should be. We were told by Giles Herdale[216] that police data is '*balkanised into proprietorial systems*', and that the technical and legal challenges are not helped by a police culture which remains well behind the curve where data is concerned.[217] This serves as a further reminder that many challenges in the investigatory powers area are not susceptible to legislative solutions.

10.8. Other issues will no doubt emerge from time to time in response to the changing nature of crime and the national security threat. It was suggested to me by one official that changes to investigatory powers law may in the future have to be contemplated with the sort of frequency associated with changes to counter-terrorism law over the past 20 years. However most of the Codes of Practice under the Act have functioned unamended since 2018,[218] and there could be few things less desirable in this area than rushed, obscure or ill-considered legislation.

---

214 See for example his remarks about the concepts of '*selection for examination*', '*secondary data*', '*by or on behalf of the operator*', '*internet service*' and '*internet communications service*' at §§16-44 of his response.

215 Response to the Review §§5-8, quoting AQOT §13.31.

216 A well-qualified interlocutor: Giles Herdale.

217 I remarked four years ago on the existence of major challenges, even within CTP, relating to capabilities, technology, disparate and sub-optimal systems, over-reliance on manual analysis of data, governance, recruitment and data standards: *2017 Terrorist Attacks, MI5 and CTP Reviews - Implementation Stock-Take* (June 2019), §5.11. Though progress is being made, it is clear that the challenges remain daunting.

218 The exception being the Interception Code, which was amended in December 2022 to support the implementation of the DAA.

The Longer Term

10.9. Previous iterations of investigatory powers law have been in force for no more than 15 years or so:[219] on that basis, it is likely that a complete replacement for the IPA will need to be in contemplation before the end of this decade.

10.10. Whereas the IPA adopted much of the terminology of its predecessor, reserving its radicalism for the areas of transparency and oversight, it is already plain that the next big law on investigatory powers will need to find a new vocabulary and a new legal framework. That framework will have to be appropriate to technology and to the threat picture as they then exist and are expected to develop; [220] it will have to be rights-compliant, while avoiding unnecessary burdens on those working in the public interest; and it will have to be comprehensible and acceptable not just to Parliament, courts and public but to the partners across national boundaries whose cooperation is likely to be ever more necessary.

10.11. Whatever procedure is devised in order to lay the ground for a major new Bill will need in my opinion to have two particularly important qualities. They may sound like nothing more than conventional modern pieties: but each of them has been shown by recent experience to be remarkably powerful in practice.

10.12. The first quality is ***diversity of input***. Crafting a successful law will not be the work of a few hands. The success of the IPA was a function of the wide range of opinion and expertise that fed into the preliminary reports,[221] their international approach, the public debate that they generated, and the rigorous pre-legislative scrutiny that enabled many changes to be made to the draft Bill before parliamentary battle-lines were drawn. The issues will be no simpler next time than they were then. A law designed for the 2030s will be made stronger and more durable by the accumulation of thoughtful, knowledgeable, constructive and honest views from practitioners, activists, policy-makers, engineers, lawyers, political leaders and interested members of the public. The voices of young people, in particular, need to be heard in relation to the technologies that will affect their lives.

---

219 Interception of Communications Act 1985; RIPA (2000). Neither RIPA nor the IPA was however a like-for-like replacement for what came before: the IPA in particular swept up a number of powers dealt with in other statutes.

220 See 2.16-2.31 above.

221 See 1.2 above.

10.13. The second quality is ***transparency*** (or as it is sometimes aptly termed in the national security field, ***translucency***): a principle whose remarkable effects were brought home to me during the passage of the IPA:

> 'The post-Snowden environment was characterised by mutual mistrust between the privacy and security lobbies, often expressed in emotional accusations: of deceit, snooping and scorn for democracy on one side, disloyalty and lack of patriotism on the other. At the root of this discord was an absence of reliable public knowledge about the true nature of intrusive capabilities that were exercised under vague and dated laws. The extensive disclosure that accompanied the draft Bill brought a measure of enlightenment to the debate. Those well-worn epithets, Orwellian and Kafkaesque, are still wheeled out from time to time, but serious commentators have moved on to serious questions: where is the operational case for this power; why should there not be further safeguards on that one. Continued and enhanced transparency, I am convinced, is the way to ensure that legislatures and courts across the world make sensible decisions in this highly contested area.'[222]

10.14. In the different context of offensive peacetime cyber operations, a former head of the NCSC and his co-author recently expressed regret over the re-emergence of what they called '*the Ronan Keating doctrine'*: the false comfort taken by some security professionals in the traditional notion that '*you say it best when you say nothing at all*'.[223] The authors called not for the disclosure of operational detail that could damage sources or methods, but for a return to the '*transformative period*' and '*remarkable form of glasnost*' that preceded the IPA.[224] Their concern over offensive cyber has now been allayed;[225] and in relation to investigatory powers the boldness of 2015 continues to pay dividends. But as practice moves on and understandings of the law adapt, the public needs to be kept informed.[226]

10.15. To take refuge in the Ronan Keating doctrine

> 'ignores the lessons the Five Eyes alliance learned painfully from the Edward Snowden leaks: that when a crisis comes, it helps if there is some general understanding in political and media circles about the sorts of activities digital spies undertake, and why.'[227]

---

222 D. Anderson, 'Shades of Independent Review' in *Counter-terrorism, Constitutionalism and Miscarriages of Justice: A Festschrift for Professor Clive Walker* (eds. G. Lennon, C. King and C. McCartney, Bloomsbury, 2018).

223 Paul Overstreet and Don Schlitz, *When You Say Nothing At All.*

224 Andrew Dwyer and Ciaran Martin, *A Frontier without Direction? The UK's Latest Position on Responsible Cyber Power*, Lawfare blog, 22 August 2022.

225 National Cyber Force, *Responsible Cyber Power in Practice*, April 2023.

226 This is the principal theme of Graham Smith's consultation response, which deplores what he calls '*the impression … of a culture of coyness in which the general public has to make do with whatever crumbs happen to fall, or be dislodged by litigation, from the table of those invited to partake*': §43.

227 Andrew Dwyer and Ciaran Martin, *op. cit.*

These words are a standing reminder that in areas of legitimate public debate, particularly where fundamental rights are at stake, silence on the part of those with privileged knowledge is a comfort zone that needs to be continuously challenged.

10.16. I am grateful to all those who have generously engaged with the Review team over the course of this Review. The openness shown from all sides was heartening: I look forward to it being reflected in any future public debates on investigatory powers.

11. LIST OF RECOMMENDATIONS

BULK PERSONAL DATASETS (Chapter 3)

BPD Issue 1: New Regime for Low/No Datasets

1. ***I recommend that IPA Part 7 should be amended to recognise a new category of BPDs in respect of which there is a low or no expectation of privacy, to which a distinct and less onerous set of safeguards should apply.*** (3.66)

2. ***Provision should be made for low/no classes to be authorised and approved via the double lock, and for any proposed low/no BPD falling outside the terms of a class to be approved by a JC as meeting the low/no criteria.*** (3.67)

BPD Issue 2: Warrant Duration

3. ***I recommend that IPA s213 be amended to provide that BPD warrants cease to have effect 12 months after they were issued, unless they have already been renewed or cancelled.*** (3.75)

BPD Issue 3: Delegation

4. ***I recommend that IPA ss202, 206, 215, 219 and 220 (but not s210) be amended so as to provide explicitly that the functions with which they are concerned may be exercised by a Crown servant on behalf of an Agency Head.*** (3.83)

INTERNET CONNECTION RECORDS (Chapter 4)

ICR Issue: Facilitating Target Discovery

5. ***I recommend that a new condition be inserted into IPA s62 allowing UKIC to obtain ICRs, if so authorised by the IPC, when it is necessary and proportionate for a national security or serious crime investigation to detect persons or devices using specific internet services.*** (4.19)

DATA RETENTION NOTICES (Chapter 5)

DRN Issue 1: Inbound Roaming Data

6. ***I recommend that IPA s87(4) be amended so as to allow DRNs to be applied for in relation to inbound roaming data.*** (5.21)

DRN Issue 2: Extraterritorial Effect

No recommendation (5.29)

CHANGES TO DEFINITIONS (Chapter 6)

Definition Issue 1: Communications Data

7. ***I recommend that the definition of communications data in IPA s261(5) is amended so that the carve-out for content does not apply in respect to subscriber data. Other related clarifications should be considered.*** (6.14)

Definition Issue 2: Lawful Authority

8. ***I recommend that a statutory definition of lawful authority to obtain CD is introduced, to include certain situations where lawful authority is currently recognised by the CD Code of Practice.*** (6.20)

Definition Issue 3: Interception

No recommendation (6.23)

TARGETED EXAMINATION WARRANTS (Chapter 7)

TEW Issue: Incidental Conduct Power

No recommendation (7.13)

WARRANTRY (Chapter 8)

Warrantry Issue 1: NCA Authorisation of TEI Warrants

9. ***I recommend that provision be made in law for senior officers of the NCA other than the Director General to authorise targeted equipment interference warrants.*** (8.10)

Warrantry Issue 2: Securing the Triple Lock

10. ***I recommend the use of a deputy to be permitted for the purposes of the triple lock when the Prime Minister is unable to approve a warrant to the required timescale (in particular through incapacity, conflict of interest or inability to communicate securely).*** (8.20)

Warrantry Issue 3: Notification on Modification of Targeted EI Warrant

11. ***I recommend that IPA s121 be amended so as to provide that s121(3) does not apply when the modification is to remove any matter, name or description included in the warrant in accordance with ss115(3)-(5).*** (8.24)

Warrantry Issue 4: Obtaining the Assistance of TOs in EI Operations

No recommendation (8.29)

OVERSIGHT (Chapter 9)

Oversight Issue 1: Appointment of Deputy IPCs

12. ***I recommend that statutory provision should be made for the IPC to nominate two deputy IPCs to whom functions currently reserved to the IPC may be delegated.*** (9.14)

Oversight Issue 2: Delegation of IPC's Functions

13. ***I recommend that deputy IPCs should have the power to appoint JCs, members of the TAP and deputy IPCs when the IPC is unable to act within the required timescale.*** (9.16)

14. ***I recommend that 'appeals' should be capable of being determined by deputy IPCs when the IPC is unable to determine them.*** (9.17)

15. ***I recommend that IPA s227(9A) be repealed*** (9.20)

Oversight Issue 3: Appointment of Temporary JCs

16. ***I recommend that deputy IPCs should have the power to appoint temporary JCs when the IPC is unable to act within the required timescale.*** (9.24)

Oversight Issue 4: Scope for Prime Ministerial Directions

17. ***I recommend that the list of bodies specified in IPA s230(1) whose intelligence-related activities may be the subject of Prime Ministerial direction to the IPC be expanded to include wider public authorities, so far as engaging in intelligence activities.*** (9.29)

Oversight Issue 5: Oversight of TROs for Prisoners

18. ***I recommend that IPA s229(3)(c) (review of TROs) be repealed.*** (9.32)

ANNEXES

ANNEX 1

LIST OF ACRONYMS/ABBREVIATIONS

List of Acronyms / Abbreviations

AI	Artificial Intelligence
AQOT	A Question of Trust (2015)
BPD	Bulk Personal Dataset
CAID	Child Abuse Image Database
CD	Communications Data
CDR	Communication Data Records
CJEU	Court of Justice of the European Union
CSA	Child Sexual Abuse
CTP	Counter-Terrorism Policing
DAA	Data Access Agreement (UK-US)
DoD	Department of Defense (USA)
DPA	Data Protection Act 2018
DRN	Data Retention Notice
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EI	Equipment Interference
EU	European Union
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation (EU)
HMRC	His Majesty's Revenue and Customs
ICO	Information Commissioner's Office
ICRs	Internet Connection Records
IPA	Investigatory Powers Act 2016
IPC	Investigatory Powers Commissioner
IPCO	Office of the Investigatory Powers Commissioner
IPT	Investigatory Powers Tribunal
IPU	Investigatory Powers Unit

ISC	Intelligence and Security Committee of Parliament
JC	Judicial Commissioner
LE	Law Enforcement
LLM	Large Language Model
MI5	Security Service
MI6	Secret Intelligence Service
ML	Machine Learning
MNO	Mobile Network Operators
MOD	Ministry of Defence
NCA	National Crime Agency
NCDS	National Communications Data Service
NGO	Non-Governmental Organisation
OCDA	Office for Communications Data Authorisations
OCG	Organised Crime Group
OTT	Over The Top
RBPR	Report of the Bulk Powers Review (2016)
RIPA	Regulation of Investigatory Powers Act 2000
RRD	Retention, Review and Disposal
RUSI	Royal United Services Institute
SIAs	Security and Intelligence Agencies (MI5, MI6 and GCHQ)
TAP	Technology Advisory Panel
TCN	Technical Capability Notice
TEW	Targeted Examination Warrant
TI	Targeted Interception
TO	Telecommunications Operator
TRO	Telecommunications Restriction Order
UKIC	UK Intelligence Community (MI5, MI6 and GCHQ)

ANNEX 2

TERMS OF REFERENCE

LIST OF SPECIFIC TOPICS

Published on 9 and 17 February 2023

Independent Review of the Investigatory Powers Act 2016

TERMS OF REFERENCE

Aim

1. To consider the priority areas for change to the Investigatory Powers Act 2016 identified as part of the cross-HMG internal strategic review to inform a potential legislative reform package to be brought forward as soon as parliamentary time allows.

Scope

2. The review should consider the operation of the Act (a) in light of the technological changes and evolving threats which have emerged over the last five years and (b) by reference to likely future developments in ways of working and technology.

3. In order to ensure that the report can be delivered in the necessary timeframe, the scope of the review should focus on the following areas identified as part of the internal strategic review (with priority given to considerations related to the Bulk Personal Dataset regime):

    a. Effectiveness of the Bulk Personal Dataset (BPD) regime and whether Part 7 remains fit for purpose;

    b. Whether changes are required to improve the effectiveness of Internet Connection Records, particularly with regard to the conditions restricting their usage set out in s62;

    c. Consideration of whether changes to definitions within the Act in relation to interception, subscriber data, and third-party data relating to the communications data retention regime are required and whether these would be practicable and desirable;

    d. Improvements to the warrantry process to increase efficiency and strengthen resilience whilst maintaining appropriate safeguards;

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

Timing

4. The Independent Reviewer should complete the review within three months (based on the timings set out in the accompanying Terms of Appointment).

Outputs

5. The Independent Reviewer should produce an unclassified final report for publication. Where appropriate, a classified annex should be produced and shared with the relevant parties. The Prime Minister will make the final decision as to whether the report, or parts of it, can be published without prejudicing the ability of the Security and Intelligence Agencies to discharge their statutory functions.

Approach and conduct of the review

6. The Independent Reviewer will lead the review supported by a DV security-cleared team and staff from the Home Office, subject to their requirements.

7. The Government and the Security and Intelligence Agencies will provide all necessary information, access and assistance as is needed for the Independent Reviewer to undertake their review effectively.

IPA REVIEW

SPECIFIC TOPICS

As an adjunct to my terms of reference, these are specific topics on which the Review invites comment during the consultation process. The Home Secretary's Statutory Report on the Operation of the Investigatory Powers Act 2016 provides the relevant context.
Whilst these are areas that have been identified as potentially needing reform in the future in the Home Secretary's Statutory Report, they are not Government policy and should not be taken as an official view on the changes necessary to ensure the Act remains fit for purpose.

1. BULK PERSONAL DATASETS (pp.14 – 15 of the Statutory Report)

a. Whether the current warrantry process in Part 7 is fit for purpose for all types of datasets

b. Whether the current duration of warrants should be amended (s213)

c. Whether certain powers vested in Agency Heads should be delegated to a Crown Servant (note that the Agency Head would remain accountable for the exercise of these functions): (ss202, 206, 210, 219, 220, 225)

2. INTERNET CONNECTION RECORDS (ICRs) - (p.17 of the Statutory Report)

a. Whether changes are required to improve the effectiveness of ICRs, particularly with regard to conditions restricting their usage (s62(3))

3. DATA RETENTION NOTICES (pp.12 - 13 of the Statutory Report)

a. Whether to address unintended consequences of s87 (4) third party data definition

b. Consider the impact of future developments in ways of working and technology on data retention capabilities

4. EXPLORE WHETHER CLARIFICATORY CHANGES TO THE FOLLOWING DEFINITIONS ARE NECESSARY (pp. 11 – 12, Pp. 18 – 19):

a. "Interception": s4(8)(a)

b. "Lawful authority": s11

c. "Subscriber data": s261

5. TARGETED EXAMINATION WARRANTS

a. Whether sections 15(5) and 99(5) should also apply to targeted examination warrants

6. WARRANTRY PROCESS (pp. 8 – 9)

a. Consider the need to provide resilience in the approval process for Targeted EI warrants, as the Director General NCA is the only law enforcement chief within the NCA who is able to authorise these warrants: s.106 and schedule 6

b. Consider the need to provide resilience in the approval process for s26 / 111 triple locked warrants where the Prime Minister is unavailable or incapacitated

c. Consider whether the process for obtaining the assistance of a telecommunications operator in equipment interference operations is efficient (s126/s128)

7. OVERSIGHT (pp. 6 – 8)

a. Consider whether amendments to the role of the IPC and wider oversight regime are required to ensure flexibility and resilience, for example including a statutory basis for Deputy IPCs, alongside the ability to appoint temporary Judicial Commissioners

DAVID ANDERSON
(LORD ANDERSON OF IPSWICH KBE KC)

17 February 2023

ANNEX 3

LIST OF CONTRIBUTORS

The following organisations and individuals responded to the Review consultation, and/or spoke to the Review Team about the issues in the Review.

BT, H3G, O2, Sky, TalkTalk,
Virgin Media, Vodafone
Neil Brown
Dame Muffy Calder, Chair of TAP
Tony Comer OBE
Counter-Terrorism Policing HQ
FCDO
Prof Craig Forcese
GCHQ
Google
Giles Herdale
Home Office (IPU)
ICO
IPCO
IPT
Mark King
Liberty
Meta
Metropolitan Police SO15
Microsoft
MI5
MI6
NCA
NCDS
NPCC
Privacy International
Dr James Renwick CSC SC
Graham Smith
Prof Peter Sommer
Turing Institute

ANNEX 4

CASE LAW DEVELOPMENTS

CASE LAW DEVELOPMENTS

1. A number of cases decided in the courts since 2016 have been relevant to the IPA. Though some have been rejected, others have resulted in changes to the Act.

Challenges to the pre-IPA regime

2. A number of organisations including Big Brother Watch applied to the European Court of Human Rights (**ECtHR**) in 2013, 2014 and 2015 to challenge the arrangements in the Regulation of Investigatory Powers Act 2000 (**RIPA**) for the acquisition of CD, bulk interception of communications and associated intelligence sharing regime. Judgments were given by a Chamber of the ECtHR in 2018 and by the Grand Chamber in 2021.[228] The Grand Chamber endorsed the use of bulk powers in principle[229] but emphasised the importance of '*end-to-end safeguards*' and in that respect identified certain deficiencies in the RIPA regime.[230] Some of these deficiencies (notably the lack of independent prior authorisation) had already been addressed by the IPA.

3. In 2015, Privacy International brought a challenge in the Investigatory Powers Tribunal (**IPT**) to other pre-IPA arrangements, separate to those contained in RIPA, for the acquisition and use by UKIC of bulk communications data (**BCD**). Privacy International also challenged the arrangements in place at that time for the use of BPD. The IPT held that these arrangements had been compatible with the ECHR since their public avowal in 2015, but that prior to that date they had not been sufficiently foreseeable to satisfy the requirements of Article 8 of the ECHR.[231] The question of whether BCD fell within the scope of EU law was referred to the Court of Justice of the EU (**CJEU**). The government accepted, after the judgment of the CJEU, that the previous arrangements for the acquisition of BCD had in certain respects not been in accordance with EU law.[232] Privacy International recently obtained permission to apply to reopen the IPT's decisions in this claim.[233]

---

228 Applications nos. 58170/13, 62322/14 and 24960/15 *Big Brother Watch & Ors v UK*, judgments of 13 September 2018 (Chamber) and 25 May 2021 (Grand Chamber).

229 The ECtHR noted that Contracting States' bulk interception regimes are *'a valuable technological capacity to identify new threats in the digital domain'* (§323) and that *'Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats'* (§347). See also §340.

230 In particular the lack of independent authorisation, the failure to require categories of selectors to be included in a warrant application, the fact that the selectors for an individual were not subject to prior internal authorisation, and insufficient protection for journalistic material.

231 IPT judgments of 17 October 2016 ([2016] UKIPTrib 15_110-CH) and 23 July 2018 ([2018] UKIPTrib 15_110-CH).

232 IPT judgment 22 July 2021 ([2021] UKIPTrib_15_110-CH).

233 This follows the IPT's recent decision in the *TechEn* litigation (see §§5-9 below) in which the IPT concluded that the Security Service had breached its duty of candour in those earlier proceedings.

Challenges to the IPA regime

4. In 2017, a wide-ranging challenge was brought by Liberty (with the National Union of Journalists intervening) to the compatibility of the IPA itself with both EU law and the ECHR. This has resulted in three Divisional Court judgments, all of which are currently under appeal.

    - Liberty challenged the compatibility of the Parts 3 and 4 arrangements for retention of CD with EU law. This challenge was upheld in 2018, in so far as Part 4 retention of CD was concerned, on the basis that access to retained data was not limited in the area of criminal justice to the purpose of detecting '*serious crime'*, and because there was no requirement of prior independent authorisation.[234] The Act was amended to remove these incompatibilities, [235] and OCDA was created to operate alongside the existing arrangements for judicial approval of warrants. Certain issues in the Part 4 EU law claim were stayed, pending a related reference to the CJEU from the IPT (§3 above).

    - Liberty challenged the compatibility with Article 8 of the ECHR of the arrangements in the IPA for the obtaining and retention of CD, equipment interference (**EI**), bulk interception of communications and BPDs. The Divisional Court rejected those challenges.[236]

    - Liberty challenged the compatibility with EU law of Parts 3 - 7 of the IPA, including the previously stayed elements of the Part 4 EU law claim. The Divisional Court held that the scheme for obtaining CD under IPA Parts 3 and 4 was compatible with EU law, save that UKIC should not be able to obtain data for the prevention, investigation or detection of crime without first making an application to the IPC. Part 7 (BPDs) did not fall within the scope of EU law, and in any event, Parts 5-7 of the Act were not '*general and indiscriminate*' so as to contravene the EU law standard.[237]

    Appeals by Liberty against aspects of these judgments are due to be heard by the Court of Appeal in May 2023. Live issues in those appeals include the question of whether the ECtHR's requirement of '*end-to-end safeguards*' applies outside the bulk interception context to other bulk powers (including BPDs); whether prior

234 *R (Liberty) v SSHD* [2018] EWHC 975 (Admin); [2019] QB 481.
235 These changes were introduced by the Data Retention and Acquisition Regulations 2018.
236 *R (Liberty) v SSHD* [2019] EWHC 2057 (Admin); [2020] 1 WLR 243.
237 *R (Liberty) v SSHD* [2022] EWHC 1630 (Admin); [2022] 1 WLR 4929.

independent approval is required before the examination of BPDs; and the level of intrusion into private life that occurs at different stages of the bulk data cycle.

TechEn

5. The *TechEn* case[238] was not a challenge to investigatory powers legislation, but to MI5's compliance with it. It requires special mention, and not only because it featured heavily in some of the consultation responses.

6. Liberty and Privacy International brought a challenge in the IPT concerning MI5's non-compliance with safeguards for the holding of warranted data, including data obtained pursuant to an IPA warrant. MI5 accepted that it failed to comply with statutory RRD requirements between 2016 and 2019, but the IPT held that there had been serious failings in compliance from late 2014 onwards, and that inadequate RRD safeguards had been in place throughout that period. Worse still, the Home Office had failed to make adequate enquiries into MI5's compliance risks from December 2016; MI5 had given assurances to the Home Office about compliance which were inconsistent with internal papers from late 2018; and the failure of the Management Board to disclose the compliance failings to IPCO until February 2019, and then only '*in unilluminating terms*', was '*a serious misjudgement*'. Accordingly, warrants issued under the IPA had been unlawful from the outset until 5 April 2019, though the IPT declined to order MI5 to delete the data obtained pursuant to those unlawful warrants.

7. In their responses to the Review, Liberty and Privacy International invited me to conclude that *'what happened in this case shows MI5 and the Home Office's complete disregard for IPA safeguards, and the ineffectiveness of those safeguards and the IPA oversight regime in practice'*. They stated that *'the fundamental flaw in this warrantry system is that MI5 (and other state bodies) are trusted to volunteer information about non-compliance to the Secretary of State, and this does not happen'*.[239] The IPT indeed found that MI5 had failed to act in accordance with its legal duties. It rejected however the broader challenge to the adequacy of the IPA oversight regime, stating:

> 'The robust steps taken by the IPC once his office had been alerted to the seriousness of the issues and investigations had been carried out demonstrates the effectiveness of the safeguards regime and the adequacy of the measures available to IPCO. There is no substance in the Claimants' assertion that the systemic failings, which MI5 had

238 *Liberty and Privacy International v Security Service and Secretary of State for the Home Department* [2023] UKIPTrib1.

239 Liberty's response to the Review at §§13-14, endorsed in Privacy International's response at §2.2.4.

failed to report or correct in accordance with its statutory duties, demonstrate that the legal regime was not in accordance with the law.'[240]

It might be added that as *TechEn* was not the first case to show, the IPT is itself a powerful safeguard, particularly when adjudicating on claims brought by skilful lawyers acting for committed and determined Claimants.

8. MI5's previous non-compliance has led to it being the subject of particularly rigorous oversight by IPCO with four extraordinary inspections taking place in 2019. The safeguards in place at MI5 now form a *'key part'* of IPCO's oversight of MI5[241] and are the subject of detailed findings in IPCO's 2020 and 2021 Annual Reports.[242] In its latest report, IPCO commended MI5's new compliance model and stated that *'given our previous investigations into compliance problems at MI5, we are hopeful that, if properly resourced, this proactive approach will ensure that any issues are identified early, if not avoided all together'*.[243]

9. While the oversight regime was not in the end found wanting and appears now to be driving significant improvement, the IPT described the episode as a '*damaging series of events*', and made a report of its findings to the Prime Minister.[244] The case is a salutary reminder of the principle underlying the IPA: that exceptional powers require strong and independent external oversight.

240 Judgment, §150.
241 IPCO 2019 Annual Report, December 2020, 8.45.
242 IPCO 2020 Annual Report, January 2022, 9.29-9.40; 2021 Annual Report, March 2023, 8.29-8.35.
243 IPCO 2021 Annual Report, March 2023, 8.4.
244 Judgment, §§193, 195.

ANNEX 5

SUBMISSION OF TONY COMER OBE

INDEPENDENT REVIEW OF THE INVESTIGATORY POWERS ACT

SUBMISSION OF TONY COMER, OBE

(GCHQ Departmental Historian 2009-2019)

The pre-computer equivalent of Bulk Personal Datasets (BPDs) have been a central part of Sigint since its inception in the First World War. Until the post-Cold War / digital comms era they can be characterised as card indexes, listing all known activity from Sigint (and from elsewhere if relevant information was available) concerning individuals. (There were lots of other indexes as well, but they aren't relevant.) During the First World War they are best known in the work of the War Trade Intelligence Department which kept an index card database of ships, mariners and traders to develop a mainly complete picture of transatlantic shipping. There is no record of what happened to the index cards after the war, but it is safe to assume that they were all destroyed.

Between the wars GC&CS was mainly concerned with diplomatic traffic. Its personality indexes (perhaps the thing that most closely resembles a BPD) though derived in part from intercept were mainly compilations of open source material. (One covers successive members of successive governments of (nearly) every country in the world and survives as a historical artefact in GCHQ.)

During the Second World War at Bletchley Park, indexes of German military and intelligence personnel were indexed and cross-referenced in a very sophisticated set of inter-related reference tools. Bletchley's hold on its sources of intelligence was always tenuous and the availability of technical equipment was always scarce, so anything that might help provide a 'way-in' to enciphered traffic was kept and meticulously indexed. For example, if Lt Schmidt, a rocket specialist at a Luftwaffe research establishment was seen in an order being posted to a unit on the French coast, it would be an indication that the unit was involved in some way in rocketry, and that therefore it would be using cryptokeys associated with the Luftwaffe's ballistic missile networks rather than (say) its bombers' network.

In the case of German intelligence personnel, the indexes provided an audit trail of how the positive identification of people referred to only by covernames had been established and enabled Bletchley Park to keep continuity on these individuals and report to MI6 to enable that agency to take active measures to counter the work of German intelligence. Material relating to intelligence personnel was always held for longer than any other intelligence targets because of the possibility that former spies might be reactivated. Some of these indexes survive to this day but have not been released, although many (though not all) of the decrypted messages which drew on them are now in The National Archives.

Similar techniques were used against the Soviet military during the Cold War, but the much larger size of the Soviet Armed Forces, and the fact that because of the lack of success by cryptanalysts against Soviet encryption systems most intelligence on the Soviet Armed Forces was produced by traffic analysis (which doesn't use the text of messages and therefore is unlikely to yield information about individuals) made them less useful.

Work against Soviet intelligence followed (and developed) the techniques used against the Germans. VENONA was a major project against Soviet intelligence messages sent in the mid-1940s and which became potentially decryptable because of errors made by the Soviets earlier. VENONA required very long-term retention of all sorts of material: the original intercepts; the worksheets which record the attempts by cryptanalysts to break individual messages; the progress of attempts to tie covernames to real people; and all of the 'collateral' – the material provided from open sources and other intelligence services which was drawn on. As the Cold War developed GCHQ in this context became more a support agency to MI5 which led in the effort against Soviet intelligence, but from the late-60s on GCHQ was able to use its technical knowledge to provide much better traffic analysis against the Soviet intelligence target than it had hitherto. The Counter Intelligence / Counter Espionage target has an important Five Eyes dimension which complicated the question of information sharing.

The same techniques were used *mutatis mutandis* by analysts working on non-Soviet targets but there tended to be more information available in publicly-available sources, which meant that indexes tended to be less comprehensive and less likely to be kept for long periods.

This is an outline of how things happened in the twentieth century before the internet age: this is why information was kept on cards, and, when PCs first became available, on databases like Access which were the fairly-direct equivalent of card indexes. The mindset of those using the indexes belongs to its period: information recording meant extracting information from documents and copying it into new documents. Retrieving information depended on all concerned sharing a single approach to recording and understanding the strengths and weaknesses of the information.

There was never any policy regarding the retention of material in these indexes: it was retained for as long as it might be needed. In the case of the German military that was up to a couple of years past the end of the Second World War. In the case of Soviet intelligence personnel and their agents it could be much longer.

3 February 2023

ANNEX 6

CASE STUDIES
(BULK PERSONAL DATASETS)

GCHQ
MI5

GCHQ CASE STUDIES

(BULK PERSONAL DATASETS)

Impact on serious and organised crime mission

1. GCHQ has an important role in reducing the harm to UK society caused by serious and organised crime. We work closely with other government departments and law enforcement partners across a wide range of high-priority topics in this area, such as countering child sexual abuse, economic crime, cyber-crime and other criminal activity. We play a key role in helping to detect and disrupt serious crime and to bring these criminals to justice.
2. The scale of the criminal threat is significant - we are increasingly searching for ways in which we can operate more effectively, maximising the impact we can have to protect the UK from that threat. We need to be able to take advantage of advances in ML to enable our analysts to react faster and to a greater number of issues.
3. However, meeting IPA requirements that apply to datasets that are widely publicly available impacts our ability to benefit from ML in the timescales we need to support operational outcomes.

Case Study

4. For example, GCHQ analysts working on an operation involving the identification of child sexual abuse (CSA) offenders received data from a partner agency to enable this important work. The dataset received was large and would have required a significant amount of time to process. ML solutions could rapidly speed up this process, to under 5% of the anticipated processing time. Had that processing been possible, we expect that offenders would have been identified faster allowing staff to make progress against a higher volume of CSA activity. To do this, we needed to train the ML model, using publicly available data. Outside of UKIC, acquiring the data would have taken a matter of hours, and training the model a matter of weeks. Due to the IPA requirements, it would have taken GCHQ weeks just to obtain the data, which made developing and training a bespoke model unviable in the context of this operation, where we needed to work at pace. Using datasets to train ML models was not foreseen when the IPA was debated, and the regime is therefore not fit for purpose for such use.
5. In this case, we could not scale our capability to this high volume, challenging target, because we were unable to take advantage of the advances in ML technology. Without changes to the current IPA requirements, we will continue to face such challenges.

Impact on capability development

6. Part of GCHQ's USP is its ability to stay one step ahead of those who would do the UK harm, which it achieves in many ways, including managing the cyber threat posed by other nation states, preventing terrorist attacks, keeping our children safe online and supporting our armed forces. Maintaining capability advantage over our adversaries is one way in which we stay one step ahead; developing and deploying new capabilities and techniques before they become widely used. This gives us a window of opportunity before hostile state actors, criminals, or terrorists learn how to counter our efforts. However, this is not easy; we are in a constant race with many others, including states with vast resources at their disposal to stay ahead. If we cannot act with speed and agility, we will likely lose our ability to develop cutting-edge capabilities that give us operational, tactical, and strategic advantages.

Case Study

7. For example, GCHQ was recently researching a new capability that would help disrupt terrorist activity. In order to make this capability an operational reality, researchers required a dataset to train a ML model. The data was essential in ensuring that the model worked effectively and in reducing the likelihood of bias. Although the data was publicly available and used widely, it constituted a bulk personal dataset under the IPA. Due to the time required to meet the safeguards, as set out in the IPA, we could not exploit a narrow window of opportunity, during which we could have secured high-value intelligence insight for months or years to come, because we were beaten to the development and deployment of the capability by others. The IPA was not designed with training ML/AI models in mind, and we are operating within frameworks that are not fit for the realities and pace of technological change that the world has seen since 2016.

MI5 CASE STUDIES

(BULK PERSONAL DATASETS)

Case Study 1	OFFICIAL Example of use of Bulk Powers
MI5 became aware of an unidentified individual whose behaviour indicated they may have been preparing themselves to conduct a terrorist attack. The individual was planning to travel to the UK and MI5 was concerned that, if the intelligence proved correct, the individual would pose a threat to UK national security and British lives could be at risk. It was imperative that MI5 fully identified the individual before they travelled to the UK, but only partial information about the individual was available. Based on this scant detail, Investigatory Powers Act provisions on bulk personal data enabled MI5 to fully identify the individual and confirm they were of national security concern. The successful identification of the individual using bulk data allowed further intelligence to be gathered, illuminating their activities and intent, and enabling a successful disruption that mitigated the terrorist threat to the UK.	

Case Study 2	OFFICIAL Example of use of Bulk Powers
The development of proportionate machine learning techniques in support of human-led investigations into individuals who pose a threat to national security is fundamental to the future operating model of modern security and intelligence services. For example, one way of detecting a threat is to train machine learning tools to find images of potential concern, such as weaponry, in datasets we have retained under the IPA. The exponential growth in volume of data in recent years means that operational datasets can be extremely large and sorting through vast numbers of images within them cannot be done manually. Machine learning tools are adept at performing this task and we need greater access to ML training/test datasets to develop these tools, which frequently qualify as BPD. This is the case even when developing tools to identify weaponry as many images of weapons will contain individuals not of investigative interest. Access to a greater volume of publicly available bulk personal datasets for model testing also helps ensure the model's efficacy and, from an ethical perspective, helps mitigate any potential biases as much as possible. By enabling a machine learning tool to be used in this context, MI5's data analysts can undertake more targeted and proportionate analysis of the results generated by the automated process and judge whether further investigation is needed. This provides greater confidence that we will detect individuals of concern in our critical investigations.	

Case Study 3	OFFICIAL Limitations of Bulk Powers
MI5 had a priority investigation into an extreme right-wing terrorism threat in the UK. MI5 had obtained a significant quantity of imagery related to this investigation, and had an urgent requirement to find an extreme right-wing terrorism-related symbol within this data. It was an investigative priority to locate this symbol within this operational dataset and extract the related intelligence.	

The quickest and most efficient method for locating the symbol was to train a machine learning model to search for it. This required obtaining a large quantity of examples of the symbol to act as the ML training dataset, helping to ensure the model's efficacy and mitigate any potential biases as much as possible. An image search for the symbol on a mainstream, open internet search site brought back many 'hits' from publicly available websites, which could have been rapidly ingested into MI5 analytical systems in an automated way to train the ML model. However, as it was possible these images could have included images of people, this meant the training dataset would be treated as a Bulk Personal Dataset (BPD).

To obtain the BPD under IPA provisions would have taken too long given the pressing investigative requirement, so instead a team of MI5 analysts had to manually search through the large quantity of imagery to find the relevant symbol and associated intelligence. This had a significant impact on the pace of not only this investigation, but on MI5's wider investigative effort, because MI5's finite analyst resource was diverted from other priorities to complete this manual task.

BPD provisions that enabled timely access to the publicly available images would have allowed a machine learning model to rapidly complete this task and respond more effectively to an immediate threat. It would have also allowed MI5's critical analyst resource to focus on other priority investigations. The impact of this friction, even where MI5 is at its most agile, means there is a cumulative drag factor on MI5's efficiency when operating under the BPD provisions in the IPA.

ANNEX 7

USERS OF BPDs
LEGAL FRAMEWORKS
(PREPARED BY HOME OFFICE)

Lord Anderson's independent review of the Investigatory Powers Act 2016

Comparable table providing an illustrative overview of the core applicable legal frameworks and regulation across different sectors who collect and analyse open-source Bulk Personal Datasets.

The use case that is consistent across all sectors centres on the collection and analysis of bulk personal datasets (BPDs) that are gathered from open sources, used within training environments to test and model machine learning/ artificial intelligence and run against live models to produce actionable intelligence.

The legal frameworks and oversight requirements illustrate the differing processing purposes, how the data is gathered and the subsequent insights and operational actions resulting from the use of BPDs.

UK Intelligence Services	National Crime Agency	Police & Law Enforcement	Commercial/ public sector
Processing purpose National Security	**Processing purpose** Law enforcement	**Processing purpose** Law enforcement	**Processing purpose** Broad spectrum of use – commercial through to identifying financial fraud (illustrative)
Applicable Law	**Applicable Law**	**Applicable Law**	**Applicable Law**
Functions Security Service Act 1989 (SSA) Intelligence Services Act 1994 **Intelligence gathering** Investigatory Powers Act 2016 Regulation of Investigatory Powers Act 2000	**Functions** Crime and Courts Act 2013 (legislation.gov.uk) **Intelligence gathering** Investigatory Powers Act 2016 Regulation of Investigatory Powers Act 2000	**Police powers and restrictive measures (non-exhaustive)** Terrorism Act 2000 Anti-terrorism, Crime and Security Act 2001 Terrorism Act 2006 Counter-Terrorism Act 2008	**Data Protection framework** UK General Data Protection Regulation (GDPR) Data Protection Act 2018 **Human rights** European Convention on Human Rights (ECHR)

Data Protection framework Data Protection Act 2018 (Part 4) **Human rights** European Convention on Human Rights (ECHR) Human Rights Act 1998 **Public Law (including both common law and legislation)**	**Data Protection framework** UK General Data Protection Regulation (GDPR) Data Protection Act 2018 **Human rights** European Convention on Human Rights (ECHR) Human Rights Act 1998 **Public Law (including both common law and legislation)**	Terrorism Prevention & Investigation Measures Act 2011 Police and Criminal Evidence Act 1984 The Passenger Name Record Data and Miscellaneous Amendments Regulations 2018 (legislation.gov.uk) National ANPR Standards for Policing and Law Enforcement **Common Law Powers** **Intelligence gathering** Investigatory Powers Act 2016 Regulation of Investigatory Powers Act 2000 **Data Protection framework** UK General Data Protection Regulation (GDPR) Data Protection Act 2018 **Human rights** European Convention on Human Rights (ECHR) Human Rights Act 1998 **Public Law (including both common law and legislation)**	Human Rights Act 1998 **Sector and regulatory targeted legislation**
Oversight	**Oversight**	**Oversight**	**Oversight**
Ministerial/Parliamentary Home & Foreign Secretary Parliament Intelligence and Security Committee of Parliament	**Intelligence gathering** Investigatory Powers Commissioner's Office (IPCO) **Use of personal data**	**Intelligence gathering** Investigatory Powers Commissioner's Office (IPCO) **Use of personal data**	**Use of personal data** Information Commissioner's Office (ICO) **Sector specific regulatory bodies**

Intelligence gathering Investigatory Powers Commissioner's Office (IPCO) **Use of personal data** Information Commissioner's Office (ICO)	Information Commissioner's Office (ICO) The ICO has agreed a voluntary arrangement to oversee NCA BPD processes.	Information Commissioner's Office (ICO) Relevant codes of practice	**Sector specific authorisation or certification schemes** **Domestic/international sector standards and regulations** **Criminal, civil and regulatory enforcement powers**
Process and/or controls	**Process and/or controls**	**Process and/or controls**	**Process and/or controls**
Data acquisition: IPA 2016 does not provide an acquisition power for BPD (only for its retention and use). BPD may be obtained via (but are not limited to): • information gateway provisions under section 2(2)(a) of Security Service Act 1989 (SSA) and sections 2(2)(a) and 4(2)(a) of Intelligence Services Act 1994 (ISA); • authorisation via other powers e.g. section 5 of ISA (property interference); section 32 of RIPA (intrusive surveillance); section 28 of RIPA (directed surveillance); and 29 of RIPA (covert human intelligence sources); • a warrant or other authorisation issued or given under the IPA 2016, where the intelligence service successfully applies to the Secretary of State to give a direction, with Judicial Commissioner approval, to disapply that regime in order to	The NCA Operating Procedure (OP) sets out the processes for managing "Bulk Personal Datasets" ("BPDs") throughout their lifecycle. The OP applies to BPDs obtained under the NCA's information gateway under **s.7 of the Crime and Courts Act 2013** and gateways under other legislation. **Data acquisition:** The NCA is not subject to Part VII IPA 2016. The NCA has a published Operating Procedure which looks to mirror safeguards found in Part VII in order to comply with Article 8 obligations. The NCA has a wide criminal intelligence function of "gathering, storing, processing, analysing, and disseminating information that is relevant to crime. BPD may be obtained via (but are not limited to): • the information gateway provisions under s.7 CCA;	No specific process requirements that are not already caught above by the applicable legislation or regulatory oversight. Policing is not subject to the IPA BPD regime. The processing of BPDs would be subject to data protection legislation and regulated by the ICO as well as any wider applicable legal regimes (e.g. Public Law duty to act reasonably etc)	No specific process requirements that are not already caught above by the applicable legislation or regulatory oversight. Private sector organisations are not subject to the IPA BPD regime. The processing of BPDs would be subject to data protection legislation and regulated by the ICO as well as any wider applicable legal regimes (e.g. a Common Law duty of confidence etc)

apply the Part 7 (BPD) regime (s.225 IPA refers) **Initial examination:** When an agency obtains a dataset, IPA provides for a preliminary examination of the contents to be undertaken to establish whether it is a BPD and assess whether the agency wishes to retain and/or examine it. The initial examination may only be carried out by an intelligence service for these limited purposes, and not for the purposes of any intelligence investigations or operations. The initial examination must take place within six months (for datasets created outside the UK) or three months (for datasets created inside the UK) from the date which the BPD was obtained. **Warrants:** Part 7 IPA provides for two types of warrant: a 'class BPD warrant' authorising an intelligence service to retain, or to retain and examine BPDs that fall within a class described in the warrant; and a 'specific BPD warrant' authorising an intelligence service to retain, or to retain and examine the particular BPD described in the warrant. Application for a BPD warrant is made to the Secretary of State by the relevant agency head. No BPD warrant may be issued unless and until the decision to do so has been approved by a Judicial Commissioner (under the 'double lock'	• acquisition via other powers but noting that acquisition of an open source low-risk BPD would generally be via the s7 CCA information gateway. **Initial examination:** When the agency obtains a dataset, the NCA OP provides for a preliminary examination of the contents to be undertaken to establish whether it is a BPD and assess whether the Agency wishes to retain and/or examine it. The initial examination may only be carried out by the NCA for these limited purposes, and not for the purposes of any intelligence investigations or operations. The initial examination must take place within six months (for datasets created outside the UK) or three months (for datasets created inside the UK) from the date which the BPD was obtained. **Warrants:** The NCA does not acquire BPDs under Part 7 IPA. The NCA OP provides for two types of authorisation for the acquisition of a BPD: a 'class BPD authorisation' authorising the NCA to retain, or to retain and examine BPDs that fall within a class described in the authorisation; and a 'specific BPD authorisation' authorising the NCA to retain, or to retain and examine the particular BPD described in the authorisation.		

warrantry process), unless a specific BPD warrant is issued under the urgency procedures. In the case of all warrants, consideration must be given as to whether the application for retention or retention and examination is necessary for one or more of the statutory grounds i.e.: in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security. It will also need to set out whether examination is necessary for one or more of the Operational Purposes specified in the warrant. The consideration of the application should also include whether the retention, or the retention and examination, of the BPD is proportionate to what is sought to be achieved; that only as much information will be obtained as is necessary to achieve those functions and purposes; and there is no reasonable alternative that will still meet the proposed objective in a less intrusive way. **<u>Examination:</u>** Once the warrant is obtained no data may be selected for examination other than in accordance with specified operational purposes, where it is necessary and proportionate.	Application for a BPD authorisation is made to the Data Authorisation Panel ('DAP') by the relevant information asset owner. No BPD authorisation may be issued unless and until the decision to do so has been approved by this panel which consists of three deputy directors (SCS 1) and on the advice of an NCA legal advisor (delegated to G6 from SCS1) unless a specific BPD authorisation is issued under the NCA OP urgency procedures. In the case of all authorisations, consideration must be given as to whether the application for retention or retention and examination is necessary for one or more of the grounds in the OP, namely: (a) for the purpose of preventing or detecting serious crime, or (b) for the purpose of preventing death or any injury or damage to a person's physical or mental health or of mitigating any injury or damage to a person's physical or mental health. It will also need to set out whether examination is necessary for one or more of the Operational Purposes specified in the application. The consideration of the application should also include whether the retention, or the retention and examination, of the BPD is proportionate to what is sought to be		

Automated systems should, where possible, be used to effect the selection for examination. UKIC should ensure that there is a system in place whereby the relevant audit or user monitoring team effectively monitors the examination of bulk personal datasets by persons with access to BPDs in order to detect misuse or identify activity that may give rise to security concerns. Section 224 of IPA makes it an offence for a person deliberately to select data for examination in breach of IPA safeguards where that person knows or believes such selection does not comply with the safeguards. **Record keeping / oversight:** Independent oversight by IPCO. The oversight regime allows IPCO to inspect BPD warrant applications and other information related to the retention and examination. UKIC must therefore keep records as detailed in the code of practice. **Review of retention and deletion:** UKIC must regularly review the operational and legal IPA and DPA justification for its continued retention, examination and use of each bulk personal dataset retained by it under a class warrant. Where the continued retention of any such data no longer meets the tests of necessity and proportionality, all copies, extracts and	achieved; that only as much information will be obtained as is necessary to achieve those functions and purposes; and there is no reasonable alternative that will still meet the proposed objective in a less intrusive way. **Examination:** Once the authorisation is obtained no data may be selected for examination other than in accordance with specified operational purposes, where it is necessary and proportionate. The BPD OP requires satisfactory safeguards to be in place, including arrangements for storing the BPD and for protecting it from unauthorised disclosure. The NCA attaches the highest priority to maintaining information security and protective security standards, including: • Physical security to protect any premises where BPDs may be accessed; • IT security to minimise the risk of unauthorised access to IT systems and BPDs, and; • A security-clearance regime for personnel to provide assurance that those who have access to BPDs are reliable and trustworthy. For each BPD there is a system in place for effectively auditing/monitoring		

summaries of it held within the relevant intelligence service must be scheduled for destruction as soon as possible once it is no longer needed for any of the authorised purposes	the examination of BPDs by NCA officers, in order to detect misuse or identify activity that may give rise to security concerns. **<u>Record keeping / oversight:</u>** The NCA has agreed with the Information Commissioner's Office ('ICO') that compliance with the data protection legislation in relation to processing bulk personal data under this OP including in relation to the authorisation, use, retention and disclosure of bulk personal datasets by the NCA, and the management controls and safeguards against misuse put in place, will be overseen by the ICO as regulator for that legislation. The ICO also has general oversight of the NCA's compliance with information rights. **<u>Review of retention and deletion:</u>** The NCA must regularly review the operational and legal justification for its continued retention, examination and use of each bulk personal dataset in line with its OP, at least every six months.		