Home Office

Report on the Operation of the Investigatory Powers Act 2016

February 2023

Home Office

Report on the Operation of the Investigatory Powers Act 2016

Presented to Parliament pursuant to Section 260(4)(b) of the Investigatory Powers Act 2016

February 2023

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at ipareviewteam@homeoffice.gov.uk

ISBN 978-1-5286-3783-1
E02825581 2/23

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

Contents

Acknowledgements

Thanks are due to officials from a wide range of government departments, agencies, and public authorities who contributed to this report, including those from:

- Security Service
- Government Communications Headquarters
- Secret Intelligence Service
- National Crime Agency
- Counter Terrorism Policing
- National Police Chiefs Council (including all regional police forces)
- His Majesty's Revenue and Customs
- Cabinet Office
- Home Office
- Foreign, Commonwealth and Development Office
- Police Service Northern Ireland
- Police Scotland
- Ministry of Defence
- Office of the Secretary of State for Scotland
- Northern Ireland Office
- Investigatory Powers Commissioner's Office

Chapter 1: Introduction and Overview of the Act

Background to the Investigatory Powers Act 2016

The Investigatory Powers Act 2016 (the Act) was introduced to replace emergency legislation passed in July 2014 (the Data Retention and Investigatory Powers Act 2014 (DRIPA)) in response to the European Court of Justice striking down the Data Retention Directive of 2006. DRIPA was subject to a sunset clause providing for the legislation to be repealed on 31 December 2016. During the passage of DRIPA, the Government committed to bringing forward new legislation which would provide the security and intelligence agencies, law enforcement and other public authorities with the investigatory powers necessary to address evolving threats within a changing communications environment.

The Act introduced world-leading oversight arrangements that strengthened the safeguards that apply to the use of investigatory powers. The Act placed the key powers on a clearer statutory footing and required warrants for the most intrusive powers to be authorised by the Secretary of State, or Scottish Minister, and for that authorisation to be approved by an independent Judicial Commissioner. The legislation is supported by statutory codes of practice on each of the key investigatory powers, providing a transparent and comprehensive legal framework.

The main aims[1] of the Act were:

- Bringing together, in a single piece of legislation, statutory powers already available to law enforcement and the security and intelligence agencies in earlier pieces of legislation to obtain communications and data about communications. It sought to ensure that these powers – and the safeguards that apply to them – are clear and understandable.
- Overhauling the way the use of the powers is authorised and overseen, introducing a 'double-lock' for warrants authorising the use of more intrusive powers – these cannot be issued by the Secretary of State or a law enforcement chief until they have been approved by an independent Judicial Commissioner. It also created the Investigatory Powers Commissioner (IPC), replacing three independent oversight commissioners, to oversee how the investigatory powers available to the intelligence services and other public authorities' powers are used.
- Ensuring the powers are fit for the digital age.

[1] Investigatory Powers Act - GOV.UK (www.gov.uk)

The Act incorporated the findings of three comprehensive reviews undertaken by Lord Anderson KC (formerly the Independent Reviewer of Terrorism Legislation)[2] ,the Intelligence and Security Committee (ISC) of Parliament[3], and a panel convened by the Royal United Services Institute (RUSI)[4]. Collectively they made 198 recommendations. All three reviews agreed that the use of these powers remained vital.

Parliamentary scrutiny of the Act included: seven separate Parliamentary reports, a separate review of bulk powers by Lord Anderson KC, the tabling of more than 1,000 amendments, and the taking of more than 2,300 pages of written and oral evidence from stakeholders across society by the Joint Act Committee alone.

The use of the powers under the Act is subject to the ongoing oversight of the Investigatory Powers Commissioner. Section 234 of the Act requires that the Investigatory Powers Commissioner makes an annual report to the Prime Minister on the operation of the Act and lays a copy of that report before Parliament. The Act requires that this report includes statistics about the use of investigatory powers, such as the number of warrants and authorisations issued, information about the operation of safeguards, and the number of errors. The Investigatory Powers Commissioner's Annual Reports are available online.[5]

Requirement to Prepare a Statutory Report

Section 260 of the Act requires that the Secretary of State prepare a report on the operation of the Act during a six-month period between May 2022 and November 2022 (five years after the Act received Royal Assent). The Act mandates that this report should take account of any other report on the operation of the Act by any Parliamentary Select Committee, and it must be published and laid before Parliament. The Home Office consulted relevant select committees ahead of preparing this report, none of whom intend to produce their own report on the operation of the Act.

Approach to the Statutory Report

This Report aims to assess, as far as possible, the extent to which the objectives of the Act continue to be met and whether any changes are required to ensure it remains fit for purpose.

When the Act was introduced in 2016, it provided vital tools for our law enforcement and security and intelligence agencies to investigate and disrupt the most dangerous criminals and national security risks. At the same time, it put in place strict safeguards to ensure they are used in a way that is both necessary and proportionate. However, it has become apparent that some elements of the oversight regime are now inhibiting the UK intelligence community's ability to work together and with partners otherwise leaving the British people

[2] A Question of Trust: report of the investigatory powers review

[3] HC 795 Intelligence and Security Committee of Parliament – Report on the draft Investigatory Powers Bill

[4] Independent Surveillance Review Publishes Report: 'A Democratic Licence to Operate' | Royal United Services Institute

[5] Annual Reports – IPCO

vulnerable to a wide range of evolving threats. This is particularly in light of Russia's invasion of Ukraine and the threat of further conflict elsewhere. The UK intelligence community has emphasised the critical importance of updating the legislation to help catch up technologically with the increasingly sophisticated tools used by terrorists, drug smugglers, and organised criminal gangs.

While the Act was designed to be technology neutral and therefore endure, a combination of technological change, the changing threat landscape (which demands new operational approaches), and legal challenges have provided cause to examine the extent to which the legislation remains fit for purpose.

The Home Office conducted an initial consultation exercise to assess the efficacy of the current legislation and to scope the options for any changes necessary to maintain and enhance that efficacy.

Engagement with law enforcement, intelligence agencies, wider public authorities and government departments found that, whilst in high level terms the Act has broadly achieved its aims, there is a case for immediate legislative change to limited parts of the Act. The initial analysis identified specific topics which warranted further exploration to ensure the operational effectiveness of the investigatory powers regime is maintained.

The earlier review provided an opportunity to consider the whole of the Act and other investigatory powers-related topics, such as challenges brought by emerging technologies. Further analysis of those topics took place to refine issues so that potential follow-on actions could be identified, including areas where legislative change may be required. The Codes of Practice pursuant to the respective powers governed by the Act have also been reviewed and will be updated in due course as required.[6]

The Investigatory Powers Commissioner's Office was engaged throughout the course of the review and this report has been shared with the Investigatory Powers Commissioner prior to publication.

[6] Investigatory Powers Act 2016 – codes of practice ; Revised Interception of Communications Code of Practice

Chapter 2: Review Outcomes

Summary of topics explored:

Oversight: Reviewed oversight of the Investigatory Powers Act 2016, including the role and remit of the Investigatory Powers Commissioner, and the respective warrantry and authorisations process.

Safeguards: Reviewed the consistency and appropriateness of safeguards across the Act.

Definitions: Assessed whether definitions of key terms in the Act remain fit for purpose.

Effectiveness of Notice Regime: Assessed how the notices provided for under the Act are managed in practice.

Bulk Personal Datasets: Reviewed the Bulk Personal Dataset regime in the context of the strategic goals for the UK set out in the Integrated Review.

Internet Connection Records: Evaluated policy and legal challenges identified through the course of ongoing trials.

Evidential Use of Data: Focused on the increasing overlap between Interception and Equipment Interference.

Oversight

The introduction of the Investigatory Powers Commissioner (IPC) and Office for Communications Data Authorisations (OCDA) was a significant change to the oversight regime provided for under previous legislation. The review provided an opportunity to demonstrate the benefits and costs of this new oversight system.

Role of the Investigatory Powers Commissioner

The IPC independently oversees the use of Investigatory Powers, ensuring that they are used in accordance with the law and in the public interest. The Commissioner is supported in his duties by the fifteen other Judicial Commissioners, the Investigatory Powers Commissioner's Office (IPCO) and OCDA. IPCO oversee the use of covert investigatory powers by more than 600 public authorities, including the UK's intelligence agencies, law enforcement agencies, police, councils, local authorities and prisons.

The Act created the role of the IPC by merging three previous independent oversight bodies: the Office of Surveillance Commissioners (OSC), the Interception of Communications Commissioner's Office (IOCCO) and the Intelligence Service

Commissioner's Office (ISComm). The Act sets out the main oversight functions of the IPC in Sections 229 (main oversight functions) and 230 (additional directed oversight functions). The IPC has a statutory obligation to report his findings and activities to the Prime Minister annually, and the report is then laid before Parliament. The IPC noted in his 2020 report that a "strong and accountable oversight model" has been established.[7]

The IPC's Remit

Maintaining and demonstrating the independence of the IPC, the Judicial Commissioners and their staff is a critical aspect of the overall Investigatory Powers framework to ensure continued public trust. The COVID-19 pandemic also highlighted the need for resilience and flexibility to be embedded within the Act to enable IPCO to manage critical incidents, such as the ability to appoint temporary Judicial Commissioners.

The government has also adjusted the IPC's functions as new areas of oversight have arisen, such as in 2020 with the Functions of the Investigatory Powers Commissioner Regulations 2020[8]. Ensuring the IPC's responsibilities remain up to date through legislation allows for the parameters of the IPC's remit to be clearly set by Parliament. The current IPC has made clear that formalising oversight responsibilities is in the best interests of transparency and robust oversight.

The review identified several pragmatic proposals for reform to the Act relating to delegation of the IPC's functions which will ensure flexibility in exceptional circumstances. These reforms are supported by IPCO and include a statutory basis for Deputy IPCs; an ability to delegate the appellate function,[9] and the ability for some Communications Data (CD) applications to be delegated to a Judicial Commissioner.

The IPC has requested that any current non-statutory functions are placed on a statutory footing and the Home Office has taken forward a statutory instrument as part of this process[10]. Some of these non-statutory functions currently include: oversight of the GCHQ 'Equities Process' (the means through which decisions are taken on the handling of vulnerabilities found in technology to achieve the best overall outcome in the interests of the United Kingdom), and oversight of law enforcement compliance in relation to the detention and interviewing of detainees overseas and the passing and receipt of intelligence relating to detainees. This is a continuation of the approach taken to the IPC's oversight of the UK-US Data Access Agreement, which was added to the list of statutory functions in 2020.

---

[7] Annual Report of the Investigatory Powers Commissioner 2020, Page 8

[8] The Functions of the Investigatory Powers Commissioner (Oversight of the Data Access Agreement between the United Kingdom and the United States of America and of functions exercisable under the Crime (Overseas Production Orders) Act 2019) Regulations 2020

[9] The ability to appeal the refusal of a warrant.

[10] The Investigatory Powers Commissioner (Oversight Functions) Regulations 2022

The review (which was limited to the subject matter of the Act) found that there is no case for systemic change to the IPC's role or current legal basis.

Warrantry and Authorisations

The warrantry process exists to provide a route for the management of warrants and authorisations for the use of investigatory powers. There are numerous mechanisms for the approval or authorisation of conduct under the Act dependent on the type of action or technique, ranging from internal authorisation for some of the least intrusive powers such as the acquisition of entity data (basic subscriber information) by the intelligence agencies, to approval by the relevant Secretary of State (SoS) and Judicial Commissioner (JC) for most targeted and bulk warrants.

The review sought to evaluate the present warrantry and communications data authorisations process to identify any challenges and inconsistencies, and to propose solutions to ensure that the system continues to function effectively and efficiently. The review identified specific 'pressure points' in the warrantry process which may ultimately require legislative change.

Access to Secretaries of State and Senior Officials

The process whereby the Secretary of State decides whether to issue a warrant, which must then be approved by a Judicial Commissioner, is known as the 'double lock'. Understandably, given the double-lock process for the approval of certain warrants under the Act, the warrantry process relies heavily on the availability of those persons authorised to issue any warrant. This naturally creates a 'pressure point' in the warrantry process.

Whenever a SoS is unavailable for any period, a backlog of routine warrants can be created. This happens most commonly when a SoS is unavailable due to recess, during election periods, or undertaking overseas travel. The same challenge arises with reference to Scottish Ministers and senior officials. These issues can be compounded by the lack of provision for some warrants to be authorised by a junior minister or senior official in urgent circumstances.

This challenge of a lack of flexibility is particularly acute for the National Crime Agency (NCA) as Director General (DG) NCA is the only law enforcement chief within the NCA who is able to authorise Targeted EI warrants (except in urgent circumstances, where an appropriate delegate may act). As currently drafted, the Act provides that warrants issued by the DG NCA may only be modified or cancelled by the DG NCA (and not by an appropriate delegate). This means that where DG NCA is unavailable these modifications cannot be authorised. This can generate delays which can have adverse impacts on operational activity.

Section 26 – the 'triple lock'

In recognition of the additional sensitivity involved, where the purpose of a warrant is to intercept the communications of a person who is a member of a relevant legislature (MRLs), the Act requires that enhanced safeguards are in place.

In addition to the 'double-lock', the Act requires that certain warrants that relate to a person who is a MRL may not be issued without the approval of the Prime Minister[11]. This is known as the 'triple-lock' as the Secretary of State's decision to issue the warrant must be approved by both a Judicial Commissioner and the Prime Minister.

The review identified an absence of deputisation provisions or powers within the Act for the Prime Minister in situations where they are incapacitated or otherwise unavailable. Further resilience may be required in legislation to account for such exceptional circumstances.

Targeted Communications Data (CD) Authorisation Process

In 2017, as part of a broader judicial review claim challenging most of the Act, Liberty[12] challenged the Communications Data (CD) provisions in Parts 3 and 4. In a 2018 judgment the High Court made a declaration that the previous lack of independent authorisation for access to certain types of CD by law enforcement and wider public authorities for serious crime purposes was unlawful. Amendments to the Act were made, introducing the Office for Communications Data Authorisations (OCDA) and a serious crime threshold.

During OCDA's first years of operation the organisation has demonstrated agility and resilience in maintaining its operations, particularly through the COVID-19 lockdown when the organisation pivoted from an entirely office-based operation to 'remote working' without significant interruption to its core business. Observations from the IPC about the performance of OCDA and statistics on applications received and authorisations granted are included in IPCO Annual Reports[13].

Public authorities are confident that applications to OCDA will likely continue to rise due to the continued importance of CD in all types of criminal investigations. Explanations public authorities have provided for the continuing increase in CD applications received by OCDA include:

- The inclusion of digital investigators within policing alongside an improved understanding of the benefits CD can bring to investigations.

[11] Section 26 and Section 111, Investigatory Powers Act 2016

[12] Liberty is the civil liberties campaigning organisation

[13] IPCO Annual Report 2020, page 36, Table 7.1

- It is now common for police forces to have a 'digital strategy' meaning digital investigations are taking over as a more efficient investigative tool than conventional surveillance, therefore the range of investigations using CD is increasing.
- OCDA's reliable response times provide confidence to public authorities that CD requests can help progress investigations in a timely manner, resulting in more requests.
- Covid-19 lockdowns resulted in an increased reliance on CD.
- Emerging technologies such as vehicle telematics and the growth in Internet of Things (IoT) devices mean that CD is available from an increasingly diverse range of sources.

UK Intelligence Community Serious Crime Targeted Communications Data Requests

The retained EU Law elements of Liberty's 2017 judicial review claim were heard during May 2022, with a High Court judgment handed down on 24 June 2022. As a result of this judgment UK Intelligence Community (UKIC) will be required to seek prior independent authorisation for targeted CD requests solely for serious crime purposes, which are currently authorised internally. The government intends to amend the Act by way of the Investigatory Powers (Communications Data) Regulations 2022 to introduce a new requirement for UKIC to obtain independent authorisation for targeted communications data requests solely for serious crime purposes from OCDA from January 2023.

Safeguards

The review of safeguards explored the consistency of safeguards and controls across the Act and the application of the protected data regime, which includes the protections applied to legally and professionally privileged material and journalistic material. The review also considered whether the safeguards remain appropriate in relation to advances in technology since 2016.

Consistency of Safeguards

Public authorities identified areas of inconsistency in the application of safeguards and controls, where there is an apparent lack of justification for the existing level of protection on certain data, which can have an impact on operational agility, and increase complexity for public authorities when interpreting the Act.

The Act doesn't expressly apply the same safeguards to all material acquired under all Parts of the Act. A specific example of this is in relation to the Bulk Acquisition of Communications Data (BCD) under Chapter 2 of Part 6 of the Act. The Act does not impose any 'confidential material' safeguards to BCD as the content of communications is never acquired. The nature of BCD also means that in many cases, UKIC will not know who data relates to at the point of selection for examination. The differing levels of intrusion associated with separate powers, and the way in which they are used in an operational context, explains many differences in the level of applicable safeguards.

In practice, overarching safeguards are applicable to the use of all powers, regardless of whether specific safeguards are imposed by the Act. Section 2 of the Act establishes "general duties in relation to privacy", in particular the duty on public authorities, when making a range of decisions under the Act, to have regard to whether particularly sensitive information should be afforded a higher level of protection. Section 2 also requires that when applying for warrants, public authorities must consider "whether what is sought to be achieved could reasonably be achieved by other less intrusive means".

The relevant Codes of Practice for BCD and for Bulk Personal Datasets ("BPD") impose safeguards for "sensitive professions"[14]. Therefore, despite the lack of specific statutory safeguards for confidential material in the safeguard provisions for BCD or BPDs, the obligation to consider a higher level of protection for this material is applied through the overarching provisions of Section 2 and the existing Codes of Practice.

Since the Act came into force, public authorities have developed a good working practice in applying the safeguards and associated thresholds. The IPC has separately corroborated this assessment, commenting on "the strong culture of compliance seen by my inspectors on their visits".[15]

Definitions

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. To ensure appropriate focus, the scope was limited to the specific definitions in the Act that define who public authorities can seek data from (for example, Telecommunications Operators), and the types of data that can be sought (for example, entity and events data).

Telecommunications Operator and Communications Data

Due to the development of the technological and commercial landscape since the inception of the Act it is not always clear whether a particular type of data or operator falls within scope of the definition of 'Communications Data' and 'Telecommunications Operator' (TO) within the Act. In practice, application of the definitions has highlighted areas of ambiguity and inconsistency. The current definitions do not always allow for the way data is now generated, stored, transmitted, or analysed. This is likely to be an increasing issue given the pace of technological change and the development of new analytical techniques. The Investigatory Powers Commissioner highlighted specific concerns with the current CD definitions in two recent Annual Reports.[16]

The Data Retention and Investigatory Powers Act 2014 expanded the definition of 'telecommunications service' to include the provision of internet-based services, such as

[14] a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, parliamentarians, or ministers of religion)

[15] Investigatory Powers Commissioner's Annual Report 2020, Page 8

[16] Investigatory Powers Commissioner Annual Report 2020, Page 90

webmail and online retail. When the Act entered into force, a further significant change was the creation of an offence in Section 11 of "knowingly or recklessly acquiring CD without lawful authority". The Investigatory Powers Commissioner noted that "although it provides an important safeguard, this offence, when combined with the ambiguity and complexity of the definition of CD, poses significant challenges for public authorities".

Most online retailers do not consider themselves to be offering a telecommunications service and therefore subject to the legal requirement to respond to a CD notice under the Act. Instead, they often insist upon reliance on the Data Protection Act. In most cases, for what are routine law enforcement requests for basic user information to assist in the detection of a crime, an authorisation for the CD element is required under the Act, and a separate request governed by the DPA for other personal data that does not amount to CD.

This has created additional bureaucracy above and beyond the intention of the safeguards introduced under the Act. The Home Office has issued interim guidance – agreed with IPCO and OCDA - for public authorities on the scope of 'CD' and on what is a 'TO' - to address these challenges. The IPC, however, believes there is a case for legislative change. The Home Office continues to work with IPCO, OCDA and operational partners to deliver a workable solution.

Effectiveness of Notices

There are several different types of notices under the Act. Data retention notices (DRNs) can be issued to mandate a telecommunications operator to retain specified communications data for a maximum period of 12 months, whereas technical capability notices (TCNs) can be issued to give effect to relevant authorisations or warrants on a perpetual basis. The review sought to assess how the Act's notice regime is managed in practice.

While both retention notices and technical capability notices are intended to be technology agnostic, the government must consider whether to be increasingly prescriptive when imposing technical requirements on TOs to ensure cost effective and efficient solutions continue to be delivered. Without the ability to levy technical requirements on TOs, or to benchmark the level of government reimbursement, there is a continuing risk that capabilities become prohibitively expensive as technology continues to evolve.

Third-Party Communications Data (Section 87(4))

Where one telecommunications operator can see or access communications data in relation to applications or services from other providers running over their network, but does not process that communications data in any way, this is regarded as third-party data.

Engagement with TOs in relation to recent changes in telecommunications standards has identified that the introduction of a new technology has brought about unforeseen

consequences. This possible impact to current CD retention could be exacerbated over time as standards and business models continue to evolve.

The risk may also materialise with the introduction of new routing technologies. There may be a need to amend the Act to provide clarity and to mitigate this risk.

Funding Model

During the passage of the Act, the existing funding model,[17] which "requires that suitable arrangements are in force for securing that telecommunications operators and postal operators receive an appropriate contribution in respect of their relevant costs as the Secretary of State considers appropriate" was subject to significant Parliamentary scrutiny and debate. UK TOs made strong representations that they should receive full cost recovery for costs associated with compliance with the provisions of the Act. The Government made commitments to reimburse 100% of the reasonable costs incurred, however, it decided not to address the exact level of contributions on the face of the Act as this was considered a matter of policy for the government of the day.

The current levels of reimbursement are based on longstanding arrangements arising from the Data Retention Regulations 2014[18] and the Regulation of Investigatory Powers Act 2000. This has seen different approaches adopted for different capabilities provided under each type of notice. For CD, the Government reimburses 100% of the capital and operational costs incurred by operators. In contrast, the Lawful Interception (LI) funding model sees TOs reimbursed for 100% of their operational costs, but reimbursement of capital costs is only for new services.

When a TO subject to a Technical Capability Notice (TCN) expands or changes its network for commercial reasons, they are expected to meet any capital costs that arise to maintain an existing LI capability. The Secretary of State has the ability, under the existing legislation, to determine what constitutes an appropriate contribution and to specify the level of reimbursement within a notice.

The Home Office is conscious of the need to secure value for money for taxpayers when imposing requirements on TOs across capabilities governed by the Act for the purposes of meeting public safety and national security requirements. There may be a future case to reassess the existing funding models to ensure consistency.

Bulk Personal Datasets (BPD)

UKIC need to retain and use a range of data from a variety of sources to meet their statutory functions, including Bulk Personal Datasets. A BPD is a set of data that has been obtained consisting of personal data relating to a number of individuals, and the nature of

[17] Section 249 provides for payments towards TO compliance costs

[18] The Data Retention Regulations 2014

that dataset is such that the majority of individuals contained within it are not, and are unlikely to become, of interest to UKIC in the exercise of their statutory functions[19].

Typically, these datasets are very large, and of a size which means they cannot be processed manually. At the time the IPA was drafted, UKIC extracted value from BPDs by asking specific questions of the data to retrieve information of intelligence value. Part 7 of the Act and the BPD Code of Practice sets out the current statutory framework, guidance and procedures governing the retention and examination of BPDs by UKIC.

Context

The Integrated Review (IR),[20] published in March 2021 and currently being refreshed, set a strategic goal for the UK to develop a competitive edge in an increasingly multipolar world through to 2030. UKIC's role in this vision is described as "being the most innovative and effective for their size in the world".[21] This followed the Spending Review 2020[22] which, in November of that year, set out the intention of the Government to "invest in the digital transformation of UKIC to further enhance their technologies and to stay ahead in an evolving digital environment".[23] The IR also set out that we are facing a period of rapid technological change, with technological developments and digitisation reshaping our societies and economies. While science and technology will bring benefits, it will also be an arena of intensifying systemic competition. This pace of change, coupled with limitations within the Act, is inhibiting UKIC's ability to maximise the benefits of digital transformation, stay ahead of adversaries, and ultimately keep the country safe. Limitations were identified through the review which will ultimately require legislative change.

The exceptional growth in volume and types of data across all sectors of society globally since the Act 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, whilst also harming capability development.

The safeguards in Part 7 do not account for the way that data and its availability has 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 cloud and commercially available tools would make powerful analysis of datasets possible;

[19] Section 199, Investigatory Powers Act 2016

[20] The Integrated Review of Security Defence Development and Foreign Policy

[21] Prime Minister's Foreword

[22] Spending Review 2020

[23] 6.42, Spending Review 2020

- 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".[24]

BPD Warrant Duration

In order to retain, or to examine and retain a BPD, UKIC must first obtain a warrant under Part 7, issued by the Secretary of State and approved by a Judicial Commissioner. A BPD warrant lasts for six months after which time it must be renewed (and every six months thereafter) if the BPD is to continue to be retained or examined. The intrusion caused by the retention and examination of BPDs is often more static and predictable than for other IPA data types where warrants authorise the continuous acquisition of data. For BPDs the data being retained and examined remains largely the same over time, so it may be appropriate for warrants to require renewal less frequently.

A longer duration of BPD warrant would also enable the value of the BPD to be more appropriately and accurately demonstrated, which in turn would provide the relevant Secretary of State with a more accurate picture of the necessity and proportionality of the continued retention, or retention and examination, of a BPD when an application for renewal is made.

Agency Head Delegation

The Act contains a number of provisions which enable certain functions to be performed by a senior Crown servant on behalf of the head of an intelligence service (an "Agency Head"). However, under Part 7 of the Act, there are certain provisions which are currently unclear in this respect.

It is not always practical or appropriate for the Agency Head to personally make decisions, statements, or technical assessments in line with the current drafting of these provisions. This issue will become more problematic as the volume of data and datasets being acquired continues to grow, as it will place more obligations directly onto Agency Heads.

Permitting the functions in these sections to be exercised by a Crown servant on behalf of the Agency Head would not undermine existing safeguards as the Agency Head would remain accountable for the exercise of these functions, even if the function were carried out by an appropriate Crown servant on their behalf; furthermore the warrant would still remain subject to the double-lock approval through a Secretary of State and Judicial Commissioner, and IPCO would continue to exercise independent oversight.

[24] IR 3.2

Internet Connection Records (ICRs)

An ICR is a record of an event held by a Telecommunications Operator about the service to which a device has connected on the internet.

The Act imposes conditions on the acquisition by law enforcement, UKIC, and wider public authorities of ICRs, or communications data that can only be obtained by the processing of ICRs.

Examples can include:

a) a record of a website visited, such as Google, but not the information that was searched for

b) a record that BBC news was visited, but not the articles that were read

c) a record that the EasyJet app was accessed on a mobile phone, but no further details about what actions were undertaken in the app or how it was used.

The CD Code of Practice sets out the additional safeguards which apply to ICRs.[25] If ICRs are sought for the investigation of crime, where the list of the records will be disclosed, the serious crime threshold[26] must be met in all circumstances. Local authorities cannot acquire ICRs for any purpose. Section 62 of the Act sets out three conditions that relate to ICRs, any one of which must always be met.

ICR Operational Use

Before any potential wider deployment of ICR retention, the National Crime Agency (NCA) has sought to trial the ICR capability through a small number of TOs. The trial has tested operational, functional, and technical aspects of a proposed approach to ICR retention, to ensure an efficient system is created which is operationally useful, ensures legal compliance and provides value for money.

The trial seeks to achieve the following outcomes:

- Testing the ability of TOs to capture and store ICR data at the necessary volume and speed.
- Assessing whether the data identified for an ICR record is sufficient and necessary for investigations, whilst also testing accuracy and quality.
- Maximising the operational benefit that can be delivered in support of investigations into serious crime.

The trial has been overseen from the outset by an IPCO inspector and is conducted on an ‘intelligence only’ basis. IPCO provide updates on the status of the trial, including the number of retention notices relating to an ICR capability, in their annual reports.

---

[25] Communications Data Code of Practice, Section 9, Page 60

[26] An offence for which an individual who has reached the age of 21 (or, in relation to Scotland or Northern Ireland, 21) is capable of being sentenced to imprisonment for a term of 12 months or more

The trial has focussed on access to websites whose sole purpose was to provide access to illegal images of children. Over 120 subjects of interest (SOIs) have been identified accessing one or more of these sites. Intelligence checks suggested that only four of these SOIs could be positively confirmed as previously known to authorities.

The scope of the review into ICRs sought to identify any policy or legal barriers through the course of the trial. The review found that some amendments could be made to the Communications Data Code of Practice to provide some clarification of oversight arrangements with potential legislative change required to the restrictions on ICRs to ensure effective use can be made of ICRs for target discovery purposes, particularly identifying Child Sexual Exploitation and Abuse (CSEA) offenders. Following the conclusion of the trial an informed decision will be taken on any approach to national service commissioning, fully considering the expected costs and benefits.

Conditions for Obtaining ICRs

Parliament imposed a high bar that must be met before an ICR authorisation can be granted. The conditions were developed as Parliament considered the balance at the time the Bill was making its way through Parliament, between intrusion into privacy, and the likely benefit that might be obtained from ICRs. The trial has now shown significant operational benefit. The way in which the conditions are drafted, and the uncertainty about how to interpret aspects of them, means that ICRs appear to be currently out of reach for some potentially key investigations, such as those seeking to identify individuals involved in some of the most serious crimes.

Evidential Use of Data

Intercept Material as Evidence

The Interception of Communications Act 1985 first put the bar on using intercept material in legal proceedings on a statutory basis. Before this date intercepted communications were generally not admitted in evidence as a matter of convention. Since 1993, eight government reviews have been commissioned to try and find a practical way to use intercept as evidence in criminal court proceedings. These include a Privy Council Review in 2008[27] with mock trials and a three-year long review between 2011 and 2014[28], overseen by Privy Councillors.

These reviews concluded that, for the use of intercept material as evidence to be consistent with the right to a fair trial (under Article 6 of the European Convention on Human Rights), all material collected by an intercepting agency in the course of a given investigation would need to be retained to an evidential standard and put in a searchable form for third parties. This would have significant privacy implications, as currently only a small amount of material useful for intelligence purposes is retained.

---

[27] Privy Council 2008 Intercept as Evidence Review

[28] 2014 HMG Intercept as Evidence Review

The last review, concluding in December 2014, estimated that the cost of implementing a legally compliant model would be £4.25-9.25bn over 20 years, depending on developing communications technology and usage, and technology costs. With the further rapid growth of internet-enabled communications, and the rise of staffing, accommodation and other expenses since these calculations were made, such costs would most likely be significantly greater now than in 2014. Aside from the high cost and practicalities involved, the previous review concluded that a legally compliant model would not meet the operational requirements of the intercepting authorities.

Following the last review in 2014, the prohibition of intercept as evidence in criminal proceedings was replicated in the IPA. Section 56 of the Act excludes from legal proceedings both material obtained under an interception warrant and anything tending to suggest that conduct under such a warrant has occurred or is going to occur. It is, however, subject to the limited exceptions contained in Schedule 3 to the IPA.

In April 2021, the High Court handed down a judgment in a judicial review brought against the prohibition on the use of intercept material as evidence in criminal proceedings as set out in Section 56 of the Act. [29] The Court concluded that the statutory bar on the use of intercept evidence in criminal proceedings is not incompatible with the European Convention on Human Rights (ECHR). The Court went on to conclude that there is therefore no basis on which a declaration of incompatibility under section 4 of the Human Rights Act could be made. The Court also concluded that there is no basis for making a declaration that the Government, or Parliament, have proceeded on the basis of an error of law as to the requirements of Article 6 (the right to a fair trial) of the ECHR.

The increasing overlap between Equipment Interference (EI) and Interception

Interception is a technique used to obtain communications where intending to make the content of them available to a person who is not the sender or intended recipient of those communications. Secondary data[30] is also obtained as a consequence of interception. Intercepted communications can include the content of a telephone call, email, or social media message, which can be intercepted in the course of their transmission; this includes interception while the data are stored on a telecommunications system (either prior to, or after, transmission).

Traditional interception was relatively simple to define and understand. Interception as defined in the IPA also provides for access to stored communications, which can cover app-based messages, emails, or texts. Stored communications can also be obtained through Equipment Interference.

A Targeted Equipment Interference (TEI) warrant authorises the interference with any equipment for the purposes of obtaining communications, equipment data or any other

[29] The Queen (On the Application of Marina Schofield) and The Secretary of State for the Home Department

[30] See sections 16 and 263 of the IPA for definitions of secondary data, which can include systems data and identifying data.

information that might otherwise constitute an offence under the Computer Misuse Act 1990.[31] TEI warrants provide lawful authority to carry out the acquisition of communications stored in, or by, a telecommunications system. Where EI activity would cause the interception of "live communications", or those which are not stored, an interception warrant must be obtained before that EI can take place. [32]

EI encompasses a broad range of techniques, from quite low-level, less sensitive capabilities, such as the use of login credentials to gain access to the data held on a computer, to more advanced capabilities. The division between the two powers in the IPA has meant that, in practice, law enforcement separates each power into separate systems. The different authorisation levels for each power has seen operational models developed on separate capabilities. This can present challenges for the 'grey area' where powers can overlap. It is also more difficult for an investigator to get an entire intelligence picture in one physical place, on one system.

The rapid growth of internet-enabled communications, even since 2016, can blur the line between communications in transit and those that are stored. Technology has moved at pace, is likely to continue to do so, and the existing EI and Interception definitions may need to be re-visited in future to ensure the Act remains up to date.

The Act governs techniques to access data, the use of different techniques to access the same data can create tension, particularly as these techniques are treated differently evidentially. Due to the existing prohibition on using intercept as evidence, only stored communications obtained in the course of conduct authorised by an EI warrant can be used as evidence.

The Act's provisions regarding the evidential use of data appear to serve public authorities well but technology will continue to advance rapidly, which may make the distinction between communications that are stored and in transit increasingly difficult to distinguish. At some stage in the future the two powers could well be combined or separated – and at that point careful consideration would have to be made about using the material as evidence. However, that is not yet required and to do so prematurely would present more practical difficulties.

[31] See section 99(2) of the IPA.

[32] See section 99(6) of the IPA.

Chapter 3: Changing Operational Environment

Technology

The Act was intentionally drafted in a technology-neutral manner to ensure that public authorities could continue to acquire operationally relevant data as technology evolved. Whilst this technology-neutral approach has largely withstood since the passage of the Act, the continued development of new communications technologies and services, which have become increasingly sophisticated and globalised, continues to affect public authorities' use of capabilities, and challenges the effective operation of the Act.

Technological changes continue to transform the challenge facing law enforcement and the security and intelligence agencies, and consequently the powers governed by the Act, with End-to-End Encryption (E2EE) and other private and secure communications technologies becoming more widespread.

Encryption

Encryption of data is now applied to most internet communications. E2EE is designed so that only the sender and recipient can know the content of a communication, rendering it inaccessible to third parties, including the service provider. The rapid evolution of internet enabled communications has seen consumers move away from the use of traditional phone calls and messaging that do not have E2EE capabilities. 70% of Over-The-Top [33](OTT) messaging application users are now using these platforms for videocalls, making access to the content of these communications encrypted and access to communications therefore more challenging.[34] Specialist Encrypted Device (SED) vendors have continued to modify commercially available smartphones to market their products towards privacy-conscious individuals. Criminals continue to attempt to use the additional security these devices provide to facilitate organised crime.

The encrypted communication service called "Encrochat" is one example of the additional challenges. Encrochat was widely used by criminals because it was considered impossible to intercept their communications. The service was compromised by European police forces using their own investigatory powers.[35] Data acquired because of the compromising of the service has led to multiple criminal prosecutions of individuals in the UK. This both illustrates the continued importance of encrypted communications to criminals as well as

[33] where a service provider delivers audio, video, and other media over an IP network (such as the internet), bypassing a traditional network operator completely

[34] OMDIA Consumer VoIP and Video Calling User and Traffic Forecast Report 2020-2025

[35] Hundreds arrested as crime chat network cracked - BBC News

the crucial nature of investigatory powers to tackle criminals using specialist encrypted services.

The UK Government supports the use of encryption, which plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security. It also serves a vital purpose to protect journalists, human rights defenders, and other vulnerable people in repressive states. However, some implementations of encryption, including other private and secure communications technologies, also pose significant challenges to public safety, including to highly vulnerable members of society like sexually exploited children, in particular severely eroding proactive child safety measures which ensure the identification and prevention of child sexual abuse online. The UK Government believes these technologies should not be applied in a way that wholly precludes lawful access to data.

The UK is not alone in this issue, and it is essential that the Government works collaboratively with like-minded governments to build consensus on the way forward, upholding public safety whilst preserving user privacy[36].

Novel Technologies

Novel technologies, including connected vehicles and Internet of Things (IoT) devices, have developed at pace over the past five years and rates of adoption will almost certainly increase. All new models of car sold in the European Union now have embedded SIM cards to contact emergency services when required. In 2016, 4.6 billion IoT devices were connected worldwide, compared to 13.8 billion in 2021.[37] Data related to connected vehicles, smart homes, and connected cities offers additional opportunities for public authorities to achieve positive operational outcomes. Successful prosecutions have incorporated smart watch, smart speaker, vehicle, and video doorbell data. In this context, law enforcement and UKIC capabilities will need to evolve to keep the UK safe.

The development of Artificial Intelligence (AI)[38] globally has seen a dramatic rise, with its use becoming increasingly pervasive across all sectors (including healthcare, transport, leisure, finance, and security). Because of its potential to transform the technology landscape, AI is recognised as a strategic priority for HMG, motivated in part to keep pace with industry, which is investing heavily in AI development.[39] GCHQ have separately published a paper on the ethics of Artificial Intelligence, which sets out that AI capabilities will be critical to the future ability to protect the UK, enabling analysts to “manage the ever-increasing volume and complexity of data” [40]. AI will not only augment what public

[36] International statement: End-to-end encryption and public safety

[37] Statista, (2021), IoT Trends 2016-2021

[38] Machines that perform tasks normally requiring human intelligence, especially when the machines learn from data how to do those tasks.

[39] National AI Strategy - GOV.UK (www.gov.uk)

[40] GCHQ | Pioneering a New National Security: The Ethics of Artificial Intelligence

authorities currently do but will likely in the future enable them to do things they would otherwise not have the resource or capability to do.

Data Overseas

More operationally relevant data is now held by service providers outside of UK jurisdiction. Shifting digital communication patterns have seen UK citizens' data no longer held exclusively by UK-based Telecommunications Operators. Data is now increasingly held by international technology providers, including cloud-based services. Data being held in overseas jurisdictions is a global challenge faced by international law enforcement, and there are global efforts through policy and legislation to mitigate this.[41]

UK-US Data Access Agreement (DAA)

The UK-US Data Access Agreement seeks to transform the ability of UK law enforcement to promptly and efficiently access data that is vital to helping keep people safe. [42] The DAA, which entered into force on 3 October 2022[43], allows UK and US law enforcement and national security agencies to directly request data held by telecommunications providers in the other party's jurisdiction for the exclusive purpose of preventing, detecting, investigating, and prosecuting serious crimes such as terrorism and child sexual abuse and exploitation.

Many of the currently popular telecommunications services, such as social media platforms and messaging services, operate within US jurisdiction. The DAA will provide relevant UK and US public authorities with timely, efficient, and lawful cross-border access to data for the purpose of preventing, detecting, investigating and prosecuting the most serious crime. It will ensure criminals cannot hide their data behind jurisdictional barriers to conceal their criminal activities.

Oversight of the DAA

Because the DAA may only be used where the correct domestic authorisation has first been obtained, all the existing mechanisms for oversight of UK investigatory powers will continue to apply. IPCO will oversee the UK's use of the DAA.

---

[41] In 2018, the United States signed the Clarifying Lawful Use of Overseas Data (CLOUD) Act, which is designed to assist US law enforcement in requesting data that is held outside of their legislation.

[42] https://www.gov.uk/government/publications/data-access-agreement-joint-statement-by-the-united-states-and-the-uk/data-access-agreement-joint-statement-by-the-united-states-and-the-united-kingdom

[43] Landmark U.S.-UK Data Access Agreement Enters into Force

Chapter 4: Conclusion and Recommendations

An overall assessment of the Act can be considered by assessing whether it has achieved its main aims and whether there have been unintended consequences. This assessment has been provided below against a summary of the aims of the Act set out in Chapter 1.

1. **Consolidation of existing powers relating to communications data, the interception of communications and equipment interference, and of oversight bodies**

This has been achieved. The introduction of the Act consolidated and updated powers which were previously provided for in a number of different statutes. Some of these Acts were enacted before the internet became a widely used means of communication so were ill-equipped for the challenges of modern technology. Bringing all these powers together under the Investigatory Powers Act 2016 helped to make the legal framework that applied to law enforcement and intelligence agencies clearer and more understandable.

2. **Enhanced oversight and safeguards for use of powers**

This aim appears to have been achieved. IPCO have released four annual reports since the creation of the oversight body and now collect a wide range of statistics on the use of investigatory powers, including those required to be published in their annual reports under Section 234 of the Act. These reports provide transparency of oversight.

IPCO carries out serious error investigations and publishes the outcomes in annual reports. IPCO has a duty to inform affected parties of a serious error under section 231 of the IPA 2016 if they judge that this is in the public interest.

The Act introduced a new offence for knowingly or recklessly obtaining communications data without lawful authority. This offence was created in order to prohibit the misuse of capabilities by public authorities and to provide additional reassurance to the public.

The Act is considered world-leading legislation that provides unprecedented transparency and substantial protection for privacy as enshrined in the UK's national and international obligations. This enhanced transparency was recognised by the UN Special Rapporteur on the Right to Privacy during a visit to the UK in 2018[44]. The UN Special Rapporteur acknowledged that the Act has significantly strengthened provisions of intelligence oversight by law, setting a new international benchmark for how the law can protect both privacy and security.

[44] UK statement for the response to the Report of the Special Rapporteur on the Right to Privacy

3. Modernisation and futureproofing

The Act was intentionally drafted in a technology-neutral manner to ensure it remained fit for purpose as technology continued to evolve. This technology neutral approach has largely withheld, however some of the issues identified through the review, such as the limitations to the BPD regime and the complexity of the communications data definitions, have shown that reform will be necessary in the short term to ensure law enforcement and the intelligence agencies can continue to effectively exercise the capabilities they need to tackle serious crime and protect national security.

Whilst the Act has largely met the initial aims of the legislation by providing for greater oversight and enhanced safeguards, and by making the powers governed by it clearer and more understandable, the review has demonstrated that the Act has not been immune to changes in technology over the last six years.

We are facing a period of rapid technological change and intensifying systemic competition. It is likely that the Act will need to be kept under review, informed by further years of operation, with more substantial reform inevitably necessary in future due to the continued unpredictability of developments in technology, and the challenges of forecasting the way that data is collected and stored against the evolving requirements of protecting national security and tackling serious crime.

E02825581
978-1-5286-3783-1