UNITED KINGDOM REPORT

Big Data Technology and National Security

Comparative International Perspectives on Strategy, Policy and Law

Law and Policy Program
Data to Decisions Cooperative Research Centre

June 2018
Research Team

Professor Louis de Koker, Program Leader
Professor Janet Chan, Project Leader
Professor Danuta Mendelson, Key Researcher
Associate Professor Lyria Bennett Moses, Key Researcher
Dr Alana Maurushat, Key Researcher
Mr David Vaile, Key Researcher
Mr Mike Gaffney, Researcher
Mr Gregory Sadler, Researcher
Mr Patrick Grierson, Researcher
Mr Daniel Cater, Project Research Assistant

Other research assistants
Ms Alana James
Ms Sonam Gordhan
Mr Jax Arnold

Interns (in alphabetical order)
Ms Kendy Ding
Mr Ciaran Finnane
Ms Monica Ma
Mr Kevin Tsu
Mr Atul Vidhata
Mr Vincent Wan
Ms Jacqueline Yip
UK Report

Authors
Chapter 1. United Kingdom: Legal and Policy Context – Louis de Koker
Chapter 2. Using Big Data For National Security: Stakeholders’ Perspectives – Lyria Bennett Moses
Chapter 3. Big Data, Law Enforcement and National Security: The Legal Environment in the UK
   3.1. Is access for data mining enabled? – Louis de Koker
   3.2. Are legal controls comprehensive and proportional? – Danuta Mendelson, Louis de Koker
   3.3. Are legal rules clear, principle-based, consistent and instructive? – Louis de Koker
   3.4. Is integrity of data and analysis supported? – Louis de Koker
   3.5. Are data and systems protected? – Louis de Koker
   3.6. Is accountability maintained? – Louis de Koker
   3.7. Are principles and rules regularly reviewed? – Louis de Koker
   3.8. Is there a sufficient measure of transparency? – Lyria Bennett Moses, Louis de Koker
Chapter 4. Conclusion
   4.1. Using Big Data for national security – Lyria Bennett Moses
   4.2. The legal environment in UK – Louis de Koker, Lyria Bennett Moses, Danuta Mendelson

Research assistance
Mr Daniel Cater
Ms Sonam Gordhan

Technical editing
Ms Sonam Gordhan
Mr David Vaile

Other Reports from this Project

Methodology Report
Australia Report
Canada Report
Comparative Report

Select Bibliography
Technical References [for Australia Report]
# Table of contents

List of Tables........................................................................................................................................... iv  
Glossary of UK terms and abbreviations................................................................................................. v  

1. UNITED KINGDOM: LEGAL AND POLICY CONTEXT ...................................................................... 1  
   1.1 Intelligence and national security – contours of the current policy discussion .................. 1  
   1.2 National security and law enforcement agencies ............................................................... 2  
   1.3 Selection of Agencies and Laws for Purposes of this Study ............................................. 5  

2. USING BIG DATA FOR NATIONAL SECURITY: STAKEHOLDERS’ PERSPECTIVES ..................... 13  
   2.1 Current use of data .................................................................................................................. 13  
   2.2 Current concerns regarding access to and sharing of data ............................................... 18  
   2.3 How problems can be overcome ......................................................................................... 20  
   2.4 Big Data: potentials, limits and risks .................................................................................. 21  
   2.5 Regulation ............................................................................................................................. 33  
   2.6 Values and Big Data ............................................................................................................. 45  

3. BIG DATA, LAW ENFORCEMENT AND NATIONAL SECURITY: THE LEGAL ENVIRONMENT IN THE UNITED KINGDOM ........................................................................ 55  
   3.1 Is access for data mining enabled? ....................................................................................... 55  
   3.2 Are legal controls comprehensive and proportional? ....................................................... 66  
   3.3 Are legal rules clear, principle-based, consistent and instructive? ................................. 80  
   3.4 Is integrity of data and analysis supported? ......................................................................... 83  
   3.5 Are data and systems protected? ......................................................................................... 87  
   3.6 Is accountability maintained? ............................................................................................... 94  
   3.7 Are principles and rules regularly reviewed? ....................................................................... 103  
   3.8 Is there a sufficient measure of transparency? ................................................................... 106  

4. CONCLUSION ..................................................................................................................................... 112  
   4.1 Using Big Data for national security: Stakeholders’ perspectives ..................................... 112  
   4.2 Big Data, law enforcement and national security: The legal environment in the United Kingdom .................................................................................................................. 119
List of Tables

Table 2-1: General Attitudes towards Computer Technology (n=5) .................................................. 13
Table 2-2: Current Concerns re Access to and Sharing of Data by Participants in Operational Organisations (n=5) ............................................................................................................... 19
Table 2-3: Conception of Big Data by Type of Organisation (n=14) .................................................. 21
Table 2-4: Perceived Capability of Big Data by Type of Organisation (n=14) .................................. 23
Table 2-5: Use of Big Data by Type of Organisation (n=14) ............................................................ 24
Table 2-6: Current Use of Data Analysis Tools by those in Operational Organisations (n=5) .......... 26
Table 2-7: Barriers/Challenges to Use of Big Data by Type of Organisation (n=14) .................. 27
Table 2-8: Risks of Using Big Data by Organisation of Research Participant (n=14) ................... 29
Table 2-9: Who is exposed to risks of Big Data by Organisation of Participant (n=14) ............ 30
Table 2-10: How Big Data Risks can be Managed (n=14) ................................................................. 32
Table 2-11: Legislation and regulatory material identified by research participants according to (1) organisation sector, and (2) type of organisation (n=14) .................................................. 34
Table 2-12: Evaluation of appropriateness and effectiveness of laws, regulation and oversight by research participants by (1) sector of organisation and (2) type of organisation (n=14) .................................................................................................................. 37
Table 2-13: Mitigation of issues/risks associated with data analytics/storage systems through design (n=2) .................................................................................................................. 44
Table 2-14: Policy participants’ attitudes to privacy by organisation sector (n=8) .................. 46
Table 2-15: Responses to general kidnapping scenario and specific prompts (n=8) ............ 47
Table 2-16: Views of research participants with policy roles on transparency of data and algorithms (n=11) .......................................................................................................................... 50
Table 2-17: Sources of views of Policy group by organisation sector ........................................... 54
Table 2-18: Control methods for types of data ................................................................................. 62
Glossary of UK terms and abbreviations

The section where a term is first mentioned is shown. See also the List of Acronyms and Abbreviations in our related Methodology Report, and Annex 1 of Anderson Report.

ACPO Association of Chief Police Officers. First mention is in heading 3.1.1.


ANPR Automatic Number Plate Recognition. See 3.1.5.

ASH All Source Hub. See 3.1.2.


BPD Bulk Personal Datasets. See Table 3-1.

CEG Communications Exploitation Group. See 3.1.2.

CESG Communications-Electronics Security Group, a part of GCHQ. See 3.5.1.

CTIRU Counter Terrorism Internal Referral Unit. See 3.1.2.


ECHR European Convention on Human Rights

GCHQ Government Communications Headquarters. See 1.2.1.

Government Response to Pre-Legislative Scrutiny Secretary of State for the Home Department (UK), Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny Cm 9219 (2016). See 1.3.2.

HMIC Her Majesty’s Inspectorate of Constabulary See 3.4.1.


IC Information Commissioner. See 1.2.3, 3.6.1.

ICO Information Commissioner’s Office. See 3.5.1.

ICRs internet connection records. See 1.1.

InSeC Intelligence Services Commissioner. See 1.2.3.

ICOCCO Interception of Communications Commissioner. See 3.6.2.

IPB Investigatory Powers Bill. See 3.1.5.


IPT Investigatory Powers Tribunal. See 1.2.3, 3.6.2.


ISC Intelligence and Security Committee of Parliament. See 1.1, 3.6.1.


ISIC Independent Surveillance and Intelligence Commission. See 3.2.1.
ISR Panel  Independent Surveillance Review Panel
JIC  Joint Intelligence Committee. See 1.2.1.

Joint Committee Report
Joint Committee on the Draft Investigatory Powers Bill, Draft Investigatory
Powers Bill Report, House of Lords Paper 93, House of Commons Paper 651,
Session 2015–16 (2016). See 1.3.2.

Lumsdon  Lumsdon & Ors, R v Legal Services Board [2015] UKSC 41; [2015] 3 WLR 121. See
3.2.7.
M15  Security Service
Miranda  Miranda v Secretary of State for the Home Department & Ors [2014] EWHC 255
(Admin); [2014] HRLR 9; [2014] 1 WLR 3140. See 3.2.7.
MLAT  mutual legal assistance treaty. See 3.1.4.
NCA  National Crime Agency. See 1.2.1
NHS  National Health Service. See 1.3.3.
NSC  National Security Council. See 1.2.1.
OSC  Office of Surveillance Commissioners. See 3.6.2.
Pham  Pham v Secretary of State for the Home Department [2015] UKSC 19; [2015] 1
WLR 1591. See 3.2.7.
PNC  Police National Computer. See 3.1.1.
PND  Police National Database. See 3.1.1.
RUSI  Royal United Services Institute. See 1.1
RUSI report  Royal United Services Institute, ‘A Democratic Licence to Operate’ Independent
SCC  Surveillance Camera Commissioner. See 3.6.1.
SIAs  Security and intelligence agencies (MI5, SIS and GCHQ). See 3.1.3.
SIS  Secret Intelligence Services (also known as Mi6). See 1.2.1.
TEU  Treaty on European Union. See 3.2.7 fn.
1. UNITED KINGDOM: LEGAL AND POLICY CONTEXT

This chapter briefly introduces the broad contours of the discussion regarding Big Data and national security in the United Kingdom. The law is reflected as at 26 May 2016.

1.1 Intelligence and national security – contours of the current policy discussion

A series of events in 2013 and 2014 led to the publication in 2015 of three key reports on surveillance powers and access to telecommunication data in the UK.

The cache of classified documents disclosed in June 2013 by Edward Snowden, a US employee of contractors for the US National Security Agency (NSA) included a large number of documents relating to the tapping by the UK Government Communications Headquarters (GCHQ) of fibre optic cables carrying important global communications. The public debate that ensued led to the establishment of two UK enquiries and also impacted on a third.

The first of these was a parliamentary inquiry launched in 2013 by the Intelligence and Security Committee of Parliament (ISC). It resulted in a March 2015 report entitled ‘Privacy and Security: A modern and transparent legal framework’ (the ‘ISC report’).

The second report was an independent review of surveillance practices in the UK. This inquiry was announced by the UK government in March 2014. The government appointed the Royal United Services Institute (RUSI), with a broad-based review panel representing senior government, industry, civil society and Parliamentary expertise, to consider broader questions regarding surveillance. These questions included advising on the legality, effectiveness and privacy implications of the UK surveillance programs, particularly as revealed by the Snowden documents; examining potential reforms to current surveillance practices, including additional protections against the misuse of personal data, and alternatives to the collection and retention of bulk data; and to assess how law enforcement and intelligence capabilities can be maintained in the face of technological change, while respecting principles of proportionality, necessity and privacy. The Independent Surveillance Report entitled ‘A Democratic Licence to Operate’ was published by RUSI in July 2015 (the ‘RUSI report’). In April 2014 the Grand Chamber of the Court of Justice of the European Union in the Digital Rights Ireland case, declared the EU Data Retention Directive invalid. The Directive provided the legal basis for UK regulations requiring service providers to retain communications data for law enforcement purposes. As a consequence of the case, the UK was under pressure to immediately adopt laws that would ensure that law enforcement and security intelligence agencies could continue to access telecommunications data needed to investigate criminal activity and protect the

---

1 See 1.2.1 for a summary of the role of GCHQ in the UK.
7 Joined Cases Digital Rights Ireland and Seitlinger and others (Grand Chamber of the European Court of Justice, C-293/12 and C-594/12, 8 April 2014).
public. To secure cross-party support enabling the fast adoption of the proposed statutory solution, the *Data Retention and Investigatory Powers Act 2014* (‘*DRIPA 2014*’) was enacted. It was agreed that DRIPA should provide for the Home Secretary to ‘appoint the independent reviewer of terrorism legislation to review the operation and regulation of investigatory powers’. The 2015 report of the Independent Reviewer of Terrorism Legislation, David Anderson QC, entitled ‘A question of trust’ (the ‘*Anderson report*’) was the result of this arrangement.

In November 2015, the UK government presented a draft Investigatory Powers Bill to Parliament. According to the Home Secretary the draft Bill, which will govern the use and oversight of investigatory powers by law enforcement and security intelligence agencies, is built on the 198 recommendations of the three enquiries. The comprehensive Bill, published for pre-legislative scrutiny, consisted of 202 sections and 8 Schedules. These outlined a new framework of powers and safeguards in relation to the interception of communications and the retention and accessing of communications data and associated activity such as equipment interference.

The Government identified the following as the key objectives of the Bill in the Bill itself:

- First, it will bring together all of the powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. It will make these powers – and the safeguards that apply to them – clear and understandable.
- Second, the draft Bill will radically overhaul the way these powers are authorised and overseen. It will introduce a ‘double-lock’ for interception warrants, so that, following Secretary of State authorisation, these – and other warrants – cannot come into force until they have been approved by a judge. And it will create a powerful new Investigatory Powers Commissioner (IPC) to oversee how these powers are used.
- Third, it will make sure powers are fit for the digital age. The draft Bill will make provision for the retention of internet connection records (ICRs) in order for law enforcement to identify the communications service to which a device has connected. This will restore capabilities that have been lost as a result of changes in the way people communicate.

This study was undertaken while public debate about the draft Investigatory Powers Bill was under way. (It passed Third Reading and proceeded to House of Lords shortly before completion of this Report.) As some of the interviewees responded to the Bill at various stages of review of the Bill, a brief outline of its progress is provided in 1.4 below.

The Bill, the debates regarding the Bill, and the three 2015 reports provide the basis for the legal and policy analysis of the UK position in Chapter 3.

### 1.2 National security and law enforcement agencies

The UK’s national security and law enforcement agencies can be divided into two groups: Intelligence and security agencies (GCHQ, MI5, SIS) and the law enforcement agencies.

#### 1.2.1 Intelligence and security agencies

Three intelligence and security agencies operate in the UK: Government Communications Headquarters (GCHQ); the Security Service (MI5), and the Secret Intelligence Services (SIS, also known as MI6).

---

The National Security Council (NSC) and the Joint Intelligence Committee (JIC) set the priorities for these agencies. They decide on their funding and also monitors their performance.  

**GCHQ:** The GCHQ gathers intelligence from communications:  

Intelligence gathering from communications may be focused on overseas, ‘upstream’ threats or – increasingly in collaboration with its sister agencies – on domestic intelligence requirements. A large proportion of GCHQ’s budget is spent on technology – including investment in capabilities developed by commercial technology companies – unusually so for a public-sector body.  

Data interception is therefore fundamental to the work of GCHQ.  

GCHQ is also the government’s lead agency on cyber-security and information assurance and on support for military operations of all types, for example by supplementing military signals intelligence capabilities.  

GCHQ works closely with MI5, supporting for example their counter-terrorism operations. It also supports the National Crime Agency (NCA) to focus on the ‘top’ organised crime syndicates and activities and the NCA’s Child Exploitation and Online Protection Command.  

**MI5:** In accordance with section 1(2) of the Security Service Act 1989, MI5’s function is ‘the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.’  

MI5 is the UK’s domestic counter-intelligence and security agency. Unlike SIS and GCHQ, MI5 does not only have intelligence gathering powers, but also has security investigative powers.  

While MI5 seeks the expertise of GCHQ where necessary, it possesses its own significant technological capabilities.  

**SIS:** SIS is the UK’s foreign counter-intelligence agency. It collects intelligence and mounts covert operations overseas in support of British government objectives.  

1.2.2 Law enforcement agencies  

The UK has 45 police forces, the largest of which is the Metropolitan Police.  

In 2013 the NCA was established as an integral part of UK law enforcement to lead the UK’s ‘fight to cut serious and organised crime’. It is positioned to have strong, two-way links with local police forces and other law enforcement and intelligence agencies.  

It combines elements of the former Serious and Organised Crime Agency, Child Exploitation and Online Protection, National Police Improvement Agency and the Metropolitan Police, and operates as a single national intelligence hub.  

---  

1.2.3 Key laws and oversight structures

The Security Service Act 1989 puts MI5 on a statutory footing while the Intelligence Services Act 1994 does the same for SIS and GCHQ.

The Human Rights Act 1998 was adopted to incorporate the fundamental rights and freedoms contained in the European Convention on Human Rights (ECHR) into UK law. It binds all bodies carrying out public functions to respect the individual rights set out in the ECHR and to ensure that their decisions comply with human rights legislation.\(^{24}\) As RUSI stated:

> In particular, decisions must be compliant with Article 8 of the ECHR, containing the qualified right to the protection of privacy:

- Everyone has the right to respect for his private and family life, his home and his correspondence
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.\(^{25}\)

The Data Protection Act 1998 provides protection to personal information and gives individuals certain rights, including the right to know what information is held about them. It also compels persons, organisations, businesses and the government to manage any personal information they hold appropriately by complying with eight data protection principles to ensure that the data is:

- Used fairly and lawfully
- Used for limited, specifically stated purposes
- Used in a way that is adequate, relevant and not excessive
- Accurate and up-to-date
- Kept for no longer than is absolutely necessary
- Handled according to people’s data-protection rights
- Kept safe and secure
- Not transferred outside the UK without adequate protection\(^{26}\)

The Information Commissioner (IC) oversees compliance with the Data Protection Act.

The Data Protection Act is subject to a national security exception. Under section 28, personal data are exempt from any of the provisions of the data protection principles, and key parts of the Act if an exemption is required for the purpose of safeguarding national security. A certificate signed by a Minister who is a member of the Cabinet or by the Attorney General or the Lord Advocate certifying that such an exemption from all or any of the relevant provisions was required for that purpose, is conclusive evidence of that fact. A person affected by such a certificate may appeal to a tribunal against the certificate.\(^{27}\)

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the powers of public bodies to carry out surveillance and investigation, including the use of undercover agents and informers. It also covers the lawful interception of communications and access to communication data and data protected by encryption. The Act furthermore empowers oversight by:

---

27 See RUSI Report 75 [4.15]: ‘An exemption from the full requirements of the DPA 1998 [Data Protection Act] exists in certain circumstances, such as where national-security interests are engaged (Section 28). The national-security exemption applies to any or all of the substantive provisions of the DPA 1998 and can be relied on so far as the exemption is required for the purpose of safeguarding national security.’
• the Interception of Communications Commissioner, who oversees the exercise of interception powers under the Act;\textsuperscript{28}
• the Intelligence Services Commissioner (InSeC), who is tasked with the review of the exercise of powers under the Act in relation to and by all three intelligence agencies;\textsuperscript{29}
• the Investigatory Powers Commissioner for Northern Ireland;\textsuperscript{30}
• the Chief Surveillance Commissioner, who functions under the Police Act 1997, to review the exercise of surveillance powers an access to protected data, in so far as they are not required to be reviewed by any of the other Commissioners functioning under the Act;\textsuperscript{31}
• the Investigatory Powers Tribunal (IPT), dealing with surveillance- and investigation-related complaints.\textsuperscript{32}

The Act also empowers the issuing of Codes of Practice,\textsuperscript{33} for example:

• Covert Surveillance and Covert Human Intelligence Sources Code of Practice 2014;\textsuperscript{34} and
• Code of Practice for the Investigation of Protected Electronic Information 2010.\textsuperscript{35}

The Justice and Security Act 2013 provides for Parliamentary oversight over the three intelligence services in the form of the ISC. The Act also provides for closed material procedure in relation to certain civil proceedings.

1.3 Selection of Agencies and Laws for Purposes of this Study

For purposes of this report, the analysis focused on the three intelligence and security agencies that operate in the UK (GCHQ, MI5 and SIS) and on two key law enforcement agencies (the Metropolitan Police and the NCA). The unique structure and operation of these agencies were however of lesser importance from an Australian perspective than their general investigatory data collection and analysis powers. The key laws outlined in 1.2.3 were considered, where appropriate, but the emphasis was placed on the implications of legislative proposals in the Investigatory Powers Bill 2016.

1.3.1 Investigatory Powers Bill

In November 2015, the government published a draft Investigatory Powers Bill that reflected many of the recommendations of the three 2015 reports.\textsuperscript{36} The Bill was published for pre-legislative scrutiny. Subsequently, in February 2016, three parliamentary committees that considered the draft Bill published reports:

The Science and Technology Committee\textsuperscript{37} considered technical aspects of the draft Bill and its impact on service providers. It made a range of recommendations emphasising the importance of

\textsuperscript{28} Regulation of Investigatory Powers Act 2000 (UK) s 57 (‘RIPA’).
\textsuperscript{29} RIPA s 59.
\textsuperscript{30} RIPA s 60.
\textsuperscript{31} RIPA s 62.
\textsuperscript{32} RIPA s 65.
\textsuperscript{33} RIPA s 71.
\textsuperscript{36} Secretary of State for the Home Department (UK), Draft Investigatory Powers Bill Cm 9152 (2015).
clarifying terminology and statutory obligations as well as close continuing engagement with industry on the likely implications of the Bill to ensure that expectations and measures are practical and that providers are able to meet the requirements within the timeframe of the Bill.38

The Intelligence and Security Committee,39 the statutory committee of Parliament that has oversight of the UK intelligence community, focused on aspects of the draft Bill which relate to the investigatory powers of intelligence agencies. Their report highlighted in particular two main areas of concern:

- Privacy protections in the draft Bill were inconsistent and needed strengthening.
  - It is the view of this Committee that privacy protections should form the backbone of the draft legislation, around which the exceptional powers are then built. Whilst recent terrorist attacks have shown the importance of the work the Agencies do in protecting us, this cannot be used as an excuse to ignore such important underlying principles or unnecessarily override them. Privacy considerations must form an integral part of the legislation, not merely an add-on.40

The Committee therefore recommended among others the inclusion of an additional section in the Act to provide universal privacy protection.

The new legislation should include a single additional Part that addresses privacy safeguards and clearly sets out universal privacy protections which apply across the full range of investigatory powers.41

- The provisions in relation to Equipment Interference, Bulk Personal Datasets and Communications Data were too broad and lacked sufficient clarity.

The Joint Committee on the Draft Investigatory Powers Bill, appointed by the House of Lords and the House of Commons to undertake pre-legislative scrutiny of the draft Bill, produced a comprehensive report.42 The committee made more than 150 observations, conclusions and recommendations.

The Investigatory Powers Bill 2016 was introduced to the House of Commons on 1 March 2016.43 The Bill, with 233 sections and 10 Schedules, was accompanied by an extensive government response to reports of the Parliamentary Committees.44 According to the Home Secretary, the Bill gave effect to the vast majority of the Recommendations made by the Parliamentary committees.45

In addition, six Codes of Practice were also published. These deal with national security notices, interception of communications, retention and use of bulk personal datasets, equipment interference, communications data and bulk acquisition.46

---

44 Secretary of State for the Home Department (UK), Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny Cm 9219 (2016).
The Bill passed the Commons in early June and faces further scrutiny in House of Lords.

1.3.2 The Investigatory Powers Bill 2016

According to the Government the Bill, which passed its Third and final Reading on 8 June 2016, will protect privacy as well as security. These protections include:

- **Increased transparency**: Statutory powers of public authorities to obtain communications or communications data are more explicit and sensitive powers that were exercised in the past are put on a clearer statutory footing. The Bill also compels the IPC to report to the public and to Parliament on the exercise of the powers.

- **Authorisation**: The Bill subjects warrants to a new ‘double lock’ mechanism requiring them to be approved by a Judicial Commissioner before they can be issued by the Secretary of State. This ensures judicial control over warrants.

- **Oversight**: The Bill combines three existing commissioners and establishes an independent IPC with new powers and appropriate resources. For example, should the Commissioner determine that a person has been the subject of a serious error, the IPC will have the ability to notify the individual concerned.

- **Limited powers**: The Bill limits the circumstances in which the powers it provides can be used. The Bill, read with the Codes, makes it clear:
  
  i. The limited number of purposes for which each of the powers in the Bill may be used.
  
  ii. The overarching human rights obligations which constrain the use of the powers set out in the Bill.
  
  iii. Whether each of the powers in the Bill must be used in a targeted way or provides for the acquisition of data in bulk. Where data is gathered in bulk, the double lock mechanism must approve the purposes for which the data can be examined.
  
  iv. The authorisation procedures that must be followed, including the review, inspection and oversight regime.
  
  v. Explicit safeguards for certain sensitive professions or categories of information (for example lawyers, parliamentarians and journalists).
  
  vi. Safeguards and obligations in respect of retention, storage and destruction of data.
  
  vii. Safeguards relating to sharing of data and material obtained under the Bill.  

- **Penalties for misuse**: The Bill must be read with other existing laws such as the *Computer Misuse Act 1990*, to clarify the circumstances in which it is an offence to obtain communications or communications data without a lawful authorisation:

  i. Interception: Interception in the absence of a warrant may constitute a criminal offence.

  ii. Communications data: The Bill creates a new offence of knowingly or recklessly obtaining communications data from a telecommunications operator or postal operator without lawful authority.

  iii. Equipment interference: The Bill preserves the current offence in the *Computer Misuse Act 1990*, so that equipment interference in the absence of a warrant will remain an offence.

1.3.3 Privacy, collection and analysis of bulk data

Many aspects of the Investigatory Powers Bill 2016 continue to be keenly debated. One element that is of particular relevance to the debate is whether the Bill provides for mass surveillance. The views

---

in this debate turn on the definition of ‘surveillance’ and whether bulk collection without human analysis or where a small amount of data is seen by human eyes constitutes surveillance. Paul Bernal put it as follows in his submission on the Bill to the Public Bill Committee of Parliament:

Precisely what constitutes surveillance is far from agreed. In the context of the internet (and other digital data surveillance) there are, very broadly speaking, three stages: the gathering or collecting of data, the automated analysis of the data (including algorithmic filtering), and then the ‘human’ examination of the results of that analysis of filtering. This is where the difference lies: privacy advocates and others might argue that the ‘surveillance’ happens at the first stage – when the data is gathered or collected – while Theresa May, David Omand and those who work for them would be more likely to argue that it happens at the third stage – when human beings are involved.48

RUSI explained the issues as follows in their report:

It is important to bear in mind that even the collection of personal data – regardless of the context in which it is collected – is considered an intrusion by some, not least because once collected the data is vulnerable to misuse or loss. However, opinions are divided as to how serious an intrusion into privacy each different stage of data acquisition, filtering, retention and eventual human analysis is. Key questions remain unanswered over the extent to which a citizen’s privacy is invaded. Aggregating data sets can create an extremely accurate picture of an individual’s life, without having to know the content of their communications, online browsing history or detailed shopping habits. ‘Given enough raw data, today’s algorithms and powerful computers can reveal new insights that would previously have remained hidden’. Some argue that to retain data at all, even if it is never analysed or only analysed by a computer, would still be unacceptable; others believe that until a human has physically examined the exact content of data then there is no intrusion. This is a debate that the public must be a part of so that a democratic consensus can be reached.49

As can be expected with such controversial legislation, the debate as to whether the Bill gets the balance right continues. On 3 May 2016 the government agreed to include general provisions submitting the discharge of the powers, duties and functions under the Bill to a range of considerations, including proportionality and necessity.50 The Labour Party and the Scottish National Party however still withheld their support. In order to address their concerns the Home Secretary agreed to order an independent review of proposed surveillance powers. The review will be conducted by the Independent Reviewer of Terrorism Legislation, David Anderson.51

---

50 The proposal included the following aspects to be considered: (a) the public interest in protecting national security; (b) the public interest in the prevention and detection of serious crime; (c) the public interest in the protection of the privacy and the integrity of personal data; (d) the public interest in the security and integrity of communications systems and networks; (e) the principle of necessity; (f) the principle of proportionality; and that no interference with privacy should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means, (g) the principle of due process, accountability and respect for the human rights of those affected by the exercise of powers under this Act; and (h) the principle of notification and redress. See Investigatory Powers Bill Debate, House of Commons, 3 May 2016 (16th sitting), 682 <http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/160503/pm/PBC_Investigatory%20Powers%2016th%20sit%20%28pm%20%29%203.5.16.pdf>.

The Joint Committee welcome[d] the introduction of a Bill as a significant step forward in human rights terms towards the objective of providing a clear and transparent legal basis for the investigatory powers already being exercised by the security and intelligence agencies and law enforcement authorities and, in many respects, enhanced safeguards.

Having examined the ‘current state of the ECHR case-law’, the Committee did not:

consider the bulk powers in the Bill to be inherently incompatible with the right to respect for private life, but capable of being justified if they have a sufficiently clear legal basis, are shown to be necessary, and are proportionate in that they are accompanied by adequate safeguards against arbitrariness.\footnote{Though it did suggest that ‘a detailed operational case for the bulk powers and recommend that it should be reviewed by the Independent Reviewer of Terrorism Legislation, who should report before the Bill completes its passage’.}

The Report made the following recommendations:

1. that the wording of the clauses concerning the subject matter of targeted interception and targeted equipment interference warrants:
   
   be amended so as to ensure that the description in the warrant is sufficiently specific to enable any person unknown, but who is the subject of it, to be identified and to prevent the possibility of large numbers of people being potentially within the scope of a vaguely worded warrant;

2. that major modifications to warrants for targeted interception be subject to approval by a Judicial Commissioner;

3. that in addition to consulting the Prime Minister, the Speaker or Presiding Officer should be notified prior to the issuance of a warrant to intercept or communications of members of Parliament, including the House of Lords, the devolved legislatures and the European Parliament. This is to provide an opportunity for these officials ‘to be represented at the hearing before the Judicial Commissioner, at which any representations could be made about matters such as the scope of the warrant, or the precision with which it specifies the matters subject to the warrant’;

4. that additional safeguards be included in provisions relating to legal professional privilege, and legally privileged items;

5. that the ‘same level of protection be provided for journalists’ sources as currently exists in relation to search and seizure under the Police and Criminal Evidence Act 1984, including an on notice hearing before a Judicial Commissioner, unless that would prejudice the investigation’;

6. the new system of oversight should provide for a clear separation of function between the prior judicial authorisation of warrants and ex post inspection and review. In particular, ‘that the Investigatory Powers Commissioner be placed under a duty to ensure that the two distinct functions of authorisation and inspection are carried out by different Commissioners’.

The Labour Party also pressed for more amendments to the Bill. On 26 May 2016, the shadow Home Secretary launched a campaign to press for changes to the Bill, raising the following matters in an open letter:

- The inclusion of an overarching privacy clause to ensure that privacy concerns raised by the Bill are adequately addressed.

\footnote{http://www.publications.parliament.uk/pa/jt201617/jtselect/jtrights/104/10403.htm#_idTextAnchor000}
• Imposing a higher access threshold restricting the use of Internet Connection Records to the investigation of serious crime, without impeding the search for missing persons and the investigation of harassment or stalking.

• Improving judicial review principles in the Bill by stipulating a clear test for review and enabling judicial commissioners to also consider the merits of the case and not just the process.

• Tightening of the provisions regarding the subsequent modification of warrants.

• Addressing the concern expressed by the National Union of Journalists that powers could be used to reveal journalistic sources, improving protection of legal privilege and ensuring Prime Ministerial sign-off on warrants involving members of Parliament.

• Allowing access to National Health Service (NHS) records to be approved only in exceptional or compelling circumstances.54

The Labour Party indicated that, unless there was significant movement by the UK Government, it would table strong amendments in each of these areas. If those were defeated and no progress was made, they would not support a timetable that will ensure that the Bill can be enacted before the DRIPA deadline on December 2016.

Civil society organisations like Privacy International,55 Big Brother Watch56 and Liberty Human Rights57 are also continuing campaigns.

1.3.4 New terminology
The distinction made by the Regulation of Investigatory Powers Act 2000 between communications data and content data became increasingly dated as technology advanced. In essence communications data under RIPA consists of traffic data, service usage information and subscriber information. Any data outside those concepts were viewed as content data.58 It was clear that these definitions had to be revised to remain relevant to new communications technologies.59

The Investigatory Powers Bill 2016 therefore defines data as including ‘data which is not electronic data and any information (whether or not electronic).’60 Data in relations to communications is then divided into two broad categories: systems data and content data.

(4) ‘[S]ystems data’ means any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any of the following:

(a) a postal service;

(b) a telecommunication system (including any apparatus forming part of the system);

(c) any telecommunications service provided by means of a telecommunication system;

(d) a relevant system (including any apparatus forming part of the system);

(e) any service provided by means of a relevant system.

(5) For the purposes of subsection (4), a system is a ‘relevant system’ if any communications or other information are held on or by means of the system.61

55 See <https://www.privacyinternational.org/node/806> for comments on the Bill on its second reading as well as <https://www.privacyinternational.org/node/865>.
56 See <https://www.bigbrotherwatch.org.uk/investigatory-powers-bill> for their general information campaign.
57 See <https://www.liberty-human-rights.org.uk>.
58 See, e.g., RIPA s 21.
60 Investigatory Powers Bill 2016 (‘IPB’).
61 IPB cl 225(4)-(5).
'Content', in relation to a communication and a telecommunications operator, telecommunications service or telecommunication system, means any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but—

(a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and

(b) anything which is systems data is not content.52

A range of new definitions are provided in relation to telecommunications and postal communications. For purposes of this discussion the most important definitions in relation to telecommunications are below.

Three concepts need to be clarified to understand the definition of communications data:

Communication, entity data (and entity can mean a person or thing)53 and events data:

‘Communication’, in relation to a telecommunications operator, telecommunications service or telecommunication system, includes -

(a) anything comprising speech, music, sounds, visual images or data of any description, and

(b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.64

‘Entity data’ means any data which—

(a) is about—
   (i) an entity,
   (ii) an association between a telecommunications service and an entity, or
   (iii) an association between any part of a telecommunication system and an entity,

(b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity’s location), and

(c) is not events data.65

‘Events data’ means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time.66

‘Communications data’, in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data -

(a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and -

   (i) is about an entity to which a telecommunications service is provided and relates to the provision of the service,

   (ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or

---

52 IPB cl 223(6).
53 IPB cl 223(7).
54 IPB cl 223(2).
55 IPB cl 223(3).
56 IPB cl 223(4).
(ii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,

(b) which is available directly from a telecommunication system and falls within sub-paragraph (ii) of paragraph (a), or (c) which -

(i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator,

(ii) is about the architecture of a telecommunication system, and

(iii) is not about a specific person,

but does not include any content of a communication or anything which, in the absence of subsection (6)(b), would be content of a communication.  

The Investigatory Powers Bill 2016 aims to clarify agency powers and protections around access to data. Chapter 3 of this report analyses how this Bill, and the legislative regime it aims to replace, provide for different aspects of the ‘lens’ set out in Chapter 5 of the Methodology Report.

---

67 IPB cl 223(5).
2. USING BIG DATA FOR NATIONAL SECURITY: STAKEHOLDERS’ PERSPECTIVES

This chapter analyses stakeholders’ responses to questions regarding their use of data, their perception of risk and challenges in relation to the use of Big Data for law enforcement and national security, and their views on the regulation of data access, sharing and retention. Terminology used to describe categories of research participants is contained in Chapter 4 of the Methodology Report. 68

The goal of this chapter is to capture understandings, perceptions and views of individual research participants on a range of issues. It is important to emphasise that the empirical findings presented in this chapter provide a snapshot of the views and perceptions of research participants only. These views and perceptions may or may not be based on a comprehensive or accurate understanding of the issues involved. Given that the sample size is relatively small and not necessarily representative of the population of stakeholders in the UK, the findings are meant to indicate issues and not to be read as a comprehensive coverage of all relevant information. We do not attempt here to evaluate or correct research participants’ views, although we have included cross-references to other sections in the report where appropriate.

Although we have used frequencies of responses throughout this chapter, these are not meant to be interpreted in terms of statistical significance. Rather, our goal is to understand the (qualitative) range of responses in particular to identify any differences from the Australian component of the study. Even there, there are necessarily views and perspectives that exist in the UK that are not captured in our study. Readers interested in the conclusions drawn from interviews, as well as the broader trends across interviews, may choose to focus on the ‘Summary and Implications’ boxes rather than the extended quotations from particular interviews.

2.1 Current use of data

2.1.1 General attitudes towards computer technology

Research participants who worked or had worked in operational organisations were asked, ‘When does digital/computer technology hinder you in your work and when is it particularly helpful?’ [03]. As can be seen from the table, there were a range of responses to this question.

Table 2-1: General Attitudes towards Computer Technology (n=5)

<table>
<thead>
<tr>
<th>Perception</th>
<th>TOTAL (n=5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both helpful and a hindrance</td>
<td>2</td>
</tr>
<tr>
<td>Helpful</td>
<td>1</td>
</tr>
<tr>
<td>A hindrance</td>
<td>1</td>
</tr>
<tr>
<td>Did not answer</td>
<td>1</td>
</tr>
</tbody>
</table>

68 The abbreviations are: O for Operational, T for Technical and P for Policy, with O/O for example representing a research participant with an operational role working in an operational organisation. Participants can have dual roles. It is crucial to note when reading this chapter that, in accordance with our project methodology, we interviewed 14 people in the UK, who were or are working in operational (5), policy (6) or independent (3) organisations. We did not interview anyone working in technical organisations, as many of these are related companies of those interviewed in Australia. Recruitment procedures for interviews were different from Australia. In Australia, we relied heavily on CRC partners to nominate people within their own organisations. In the UK, we relied on diplomatic assistance as well as local professional and personal contacts. Differences in recruitment methods, fieldwork time frame, and individual willingness to participate mean that the sample of UK interviewees may not be directly comparable to the Australian one. In particular, three of the five research participants in operational organisations in the UK worked on trend identification, program strategy and evaluation teams rather than in direct investigation or intelligence roles. While some of the Australian participants were not in direct investigation or intelligence roles, this represented a smaller proportion.
Helpful. Digital and computer technology was viewed as helpful in the sense that it was ‘essential for what we do’ (O-T/O A). Digitisation was a particularly important development for intelligence — one research participant reflected on a time when ‘you could already see that the digitisation of communications and the digitisation of stored data was going to revolutionise the way intelligence activity was conducted, quite apart to what it would do to government in providing information for policy making.’ (O-P/O B)

Hindrance. A significant hindrance in the UK, reflected in comments of all three research participants who commented negatively, seemed to be with the age of computer systems, which were described as inflexible and not designed for current needs or ‘archaic’ (O-T/O C):

[T]here’s a myriad of systems because we have 43 different police forces not all using the same system. ... Also it’s the lack of central government’s ability to be agile in using the latest technology. So we sign ourselves ... into contracts with organisations that aren’t flexible enough. If you want to make any changes it costs huge sums of money. (O-T/O D)

The computer systems that [Law Enforcement Agency] have are ancient, it’s still on Internet Explorer 6 or something, you can’t even get on a [particular agency] website on a [Law Enforcement Agency] machine. (O-T/O E)

[Databases] were built to store data rather than take it out and use it; that is a massive hindrance (O-T/O F).

Summary and Implications

While all computer systems are built around current needs and use cases, it is important to bear in mind the need for flexibility in design and in contracts, so that systems can be adapted to meet future needs over time. Computer systems need to be ‘up to date’ in order to perform what may come to be regarded as basic functions.

2.1.2 Types of data used

We asked all participants from operational organisations, ‘What types of data do you (or your unit) use in your work?’ [O4] This is a very broad question that elicited a wide range of answers, depending on participants’ own perception of what ‘data’ is and the nature of their organisation. Our discussion represents what participants told us in interviews—they do not constitute a comprehensive inventory (impossible given the number of participants in this category). Further, because we are adopting the terms used by research participants, categories may overlap or coincide.

Two research participants mentioned using ‘crime data’, a category that was described as including Crime Recording Information System, Police National Computer, Electronic Warrant Management System, Trident Gang Command Matrix, databases containing data on complaints about police, police misconduct, calls to police, prosecutions, and court proceedings. Despite the centralisation in the Police National Computer (PNC) (see 3.1.1), some types of ‘crime data’ were described as being held across multiple databases without automated processes to bring datasets together.

‘Intelligence data’ as a broad category was mentioned by two research participants. Other types of data mentioned included:

- data about offenders (including employment, welfare and education data),
- data about targets,
- ‘raw information’, described as ‘the whole web, every person’s phone billing, everything’
- social media data such as Twitter, which was also mentioned in the Anderson report as an increasingly important category69

---

• human intelligence,
• signals intelligence,
• protected personal data intelligence
• evidence,
• data on missing persons,
• child custody data (which a different participant mentioned was separate from criminal justice data), and
• digital data or digital intelligence, described as including both ‘data at rest’ such as passport databases, vehicle databases, passenger information, hotel records, bank records and open source data, as well as ‘data in motion’ or communications data.

The research participant who mentioned digital data or digital intelligence divided this category into three types:

... I suppose there’s a broad distinction between the databases to which you lawfully have access either through domestic law, government or private sector such as banks or lawfully can access by means of an agreement with your partners. So for example DNA databases in Europe and the [Schengen] convention. Or databases you have stolen such as somebody else’s passport database. ... so small country X in the centre of some crisis zone with Jihadists doing nasty things, can you get hold of ... their passport database and thus try and identify whether people are masquerading as things they shouldn’t be ... (O-P/O A)

Two research participants (O-T/O) also mentioned a desire to access health data, in one case in relation to offenders (for example, in relation to drug treatment) and in the other in relation to victims (for example, stabbing and shooting victims).

**Summary and Implications**

As in Australia, research participants in the UK used broad categories to describe the data that they used, while others focussed on particular databases. One interesting observation, however, was the fact that, despite the centralisation in the Police National Computer (see 3.1.1), some types of crime data are held across multiple databases without automated processes to bring datasets together.

2.1.3 Types of data generated

This question was deliberately omitted from the UK study.

2.1.4 Sharing of data

We asked research participants who were working or had worked in operational organisations ‘Does your agency/unit share data with other agencies and, if so, which ones?’ [O5] and ‘What kind of data is shared – is it raw or summarised; identified or de-identified?’ [O6]. As in Australia, data in the UK is made available to other agencies (including international partners), and in some cases on an aggregated basis to the public.

**Types of data shared**

- **Intelligence reports.** As in the case in Australia, intelligence is often shared in reports, which may include raw, identified but limited/curated data about a target (O-P/O) or may comprise ‘assessed intelligence’ (O-T/O).

- **Open data.** Two research participants from the same organisation (both O-T/O) described ‘performance dashboards’ based on aggregate or de-identified data that were made available (mostly to researchers) through the UK data archive, also known as the ESX data store. Another research participant described how aggregate data was released to the public
through reports, with the risk of re-identification of individuals reduced through testing conducted prior to release of the data (O-T/O).

**Conditions for sharing.** Interviews revealed different arrangements for those working directly on operational matters, compared to those responsible for research and evaluation on operational programs.

- **Human-mediated and controlled by legislation.** One research participant, from an intelligence agency, described a human-mediated but broad sharing regime among operational agencies:

  [E]ssentially the view is taken it’s all the Queen’s data. So the basic presumption is if there’s an operational need to share it, and the responsibility is on the agency with the data to think about who might be able to use it, then it gets shared. ... The legislation contains quite strict instructions on disclosure and the conditions under which it can be shared. [Q: Each agency will maintain its own data store?] Yes. [Q: Which the other agencies don’t just access directly?] No. ... There are some government databases, vehicle licencing database for example which is accessible both by the police and by the security service. ... [T]here is a great deal of data sharing but it is human controlled as much for security purposes and to some extent for legal propriety if you’re talking about court material which will end up in court. (O-P/O A)

- **Relevance.** Two research participants working in or with law enforcement confirmed that data sharing was not unrestricted:

  We are sharing what is relevant, not all data. (O-T/O B)

  We only share on relevant targets to relevant teams. Because of volume, agencies only share what is required, we are not making them store irrelevant information. Also this kind of sharing is what the information commissioner wants. We are only keeping and storing what is relevant and what meets all legal processes. Raw information would not be shared with other agencies. Much more assessed intelligence that we are sharing. There is very little of any sharing of a whole lot of information. What would have been a manual process before, we are just doing it in bulk. ... Only if identities are relevant to that team do we share them. (O-T/O C)

- **Proportionality.** One research participant, working with crime and offender data, described how the fact that ‘we work on the principle of proportionality’ meant that ‘it has to be a very clear rationale, not a fishing expedition’ and that where data was shared between government departments, the least amount of data possible was shared to facilitate cross-linking:

  If I have 20 million individuals on my data set and somebody in another government department wants to look at the 100,000 people they have on theirs, I won’t give them 20 million. They’ll give me 100,000, I will pull out the information that is applicable to the work that they’re doing, and share that with them. ... [I]t won’t be necessarily a full suite of information that they hold, it is what has been agreed as part of the rationale for the work you’re doing. (O-T/O D)

Given this research participant worked in research and evaluation, rather than a directly operational role, it would seem that (at least in that context), the amount of data shared is minimised, so that the least amount of data is shared to facilitate a clear purpose. In operational contexts, a principle of data minimisation may not apply, as where the Police National Computer facilitates automatic sharing of data across law enforcement agencies.

- **Open access.** This approach did not seem to be universal. Another research participant in an agency doing research on law enforcement data had ‘no firewall between us and police data’.
• **Inter-agency agreements.** Two research participants described data sharing agreements or memoranda of understanding as the basis for data exchange between agencies:

There were a variety of security concerns that we worked through, in terms of getting individuals trained, the appropriate level of vetting, using the appropriate levels of security ... (O-T/O E)

So everything is either memorandum of understanding or a data sharing agreement, which stipulates in quite a lot of detail what can and cannot be done, and even to some extent who, as in named individuals, can and cannot have access to the information. ... In general it’s a separate one each time [data is shared]. For certain ones where we are trying to do this on a regular basis, we are trying to have a standard one that is more an annual review. (O-T/O F).

• **International sharing.**70 As in Australia, sharing internationally is highly curated. There are different memoranda of agreement with different international partners (O-T/O). In the case of Five Eyes, ‘signals intelligence agencies are sharing much of their raw intercept among themselves ... If you took the human intelligence agencies, you would not find that. You would find sharing is human controlled and piece by piece depending on the circumstance.’ (O-P/O G). In the UK, distinctions are drawn based on the location of the data subject rather than citizenship:

[Y]ou’ve got a different set of regimes where it rather depends on what kind of information it is. Information about [people in the British Isles] for example is shared, but is shared with caveats about no use may be made of this data without reference back et cetera. ... [G]reat care is taken to protect if you like the data of persons in the British Isles and there are separate arrangements for authorising for example interception of persons in the British Isles as against people overseas. (O-P/O H)

**Summary and Implications**

As in Australia, data sharing is a highly curated process with different rules for different agencies, often worked out through negotiated agreements. In many cases, reports are shared rather than access granted to raw data or databases. Aggregated data may be made available to the public, sometimes in innovative ways (such as interactive dashboards).

One noteworthy element of UK data sharing arrangements is that the principle of proportionality seems to have an impact on data sharing arrangements among government departments, particularly for research and evaluation rather than directly operational concerns. In particular, the amount of data shared may be minimised, so that the least amount of data is shared to facilitate a clear purpose.71 However, much crime data is shared automatically through the use of shared databases such as the Police National Computer.

---


71 IPB institutionalises this practice through the filter mechanism; see IPB cl 58: Filtering arrangements for obtaining data; cl 59: Use of filtering arrangements in pursuance of an authorisation, and cl 60: Duties in connection with operation of filtering arrangements.
targets and ... to discover new threats’ (O-P/O); ‘building a strategic picture’ (O-T/O) and national security (O-P/O).\textsuperscript{72}

One purpose that came up in the UK that was not mentioned in the Australia study (perhaps due to anomalies in recruiting research participants in each jurisdiction) was research on trends and program evaluation, which can then be used by government for strategic decision-making so that money is not spent on ineffective programs (O-T/O). While this might overlap with ‘policy making’ which came up in the Australian study, the descriptions were more specific:

If you’re going to fund [intervention in emergency rooms to prevent reoffending] to a million pounds you might wish to know what the outcome of that is. You could spend that million pounds in another way if it doesn’t make any difference. (O-T/O A)

So what happens in a court doesn’t seem to impact on what happens in a prison, even though there will be crossover between the two sets of people. So part of my role is to bring all of these together and also add on other data information from other government departments. So educational attainment from Department for Education, or higher education information from BIS - Business, Innovation and Skills, earnings and data from ... the Department for Work and Pensions or the revenue system. So bringing all of that together to understand drivers on offending. (O-T/O B)

A big chunk of [our work is around] performance ... [it has] seven key crime types that it follows. It has other key confidence targets, measures around criminal justice issues, youth reoffending. We use the data ... to assess, and measure all of those areas, look at if we’re meeting the targets, projections, which [regions] are particularly bad. Really delve into the detail a lot, and that’s for external work [public release] and also internal performance, internal strategy, internal monitoring. ... The second chunk of our work is around research, so we conduct a whole host of research, ranging from process evaluations, all the way up to ad hoc analytics, all the way to experimental designs. ... We conduct a variety of large scale ... surveys ... [O]ne of the things I’m really keen is blending together performance data next to social research data. (O-T/O C)

\textbf{Summary and Implications}

In the UK, apart from the use of data for crime prevention, criminal investigation and security intelligence, research participants reported using crime and offender data to conduct research on offending trends and to evaluate criminal justice programs. It is possible that evidence-based policy in criminal justice research is more developed in the UK than in Australia, although further investigation into the Australian situation would be required to draw any conclusions given differences in sample composition between the two studies and the small sample size.

\section*{2.2 Current concerns regarding access to and sharing of data}

Participants from operational organisations were asked, ‘What are your major concerns in relation to data access from other agencies or sharing data with other agencies?’ [O7]. Table 2-2 summarises the responses to this question, which fall into the same categories as the responses in Australia.

We also asked ‘Do these problems affect your (or your staff’s) morale or sense of professionalism?’ The responses indicated frustrations or annoyance and negative impact on insights that can be gained (O-T/O), but no research participants suggested there were issues for morale or professionalism.

\textsuperscript{72} See also Intelligence and Security Committee, \textit{Privacy and Security: A modern and transparent legal framework}, House of Commons Paper 1075, Session 2014-15 (2015) 3 [vii]. Unlike in Australia, ‘national security’ is not defined in the legislation, because of its evolving nature (see 3.3). One research participant defined it as ‘It’s all the very major threats to the everyday life of the public rather than the protection of the state and from external attack and prevention of subversion which would be a kind of 20th century definition of national security.’ (O-P/O)
Table 2-2: Current Concerns re Access to and Sharing of Data by Participants in Operational Organisations (n=5)

<table>
<thead>
<tr>
<th>Concern</th>
<th>TOTAL (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal requirements/privacy – real or perceived</td>
<td>5</td>
</tr>
<tr>
<td>Technical issues</td>
<td>5</td>
</tr>
<tr>
<td>Ownership and trust</td>
<td>3</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant.

2.2.1 Real or perceived legal requirements

As in Australia, general privacy legislation and rules around particular datasets (such as health data) posed a barrier to data sharing. Given the requirement for data sharing agreements or memoranda of understanding between agencies, one interviewee contended that significant time may be required to establish access to new data sets (O-T/O). Another mentioned an example where the agency that held the data suggested that they use a freedom of information request to access particular data, as that was ‘the easiest way we can give it to you’ (O-T/O). We are not aware as to whether there are similar uses of freedom of information laws in Australia.

One international restriction on sharing data mentioned was the ‘third party rule’ whereby data that has been shared once is not shared with anyone else without reference to the originator (O-P/O). Another is the risk that the agency with whom information is shared will act on it and compromise a British operation (O-P/O). In addition, ‘there are always some areas you don’t share on’ due to national sensitivities (O-P/O).

2.2.2 Technical issues

As in Australia, technical concerns include the lack of an integrated system as well as the difficulty (given the lack of single a national identifier) of linking information across databases. One research participant raised the issue of data security, particularly in the case of sharing information about people in the British Isles with foreign intelligence agencies (O-P/O). Another research participant mentioned the difficulty of extracting data from databases that were designed primarily to store data (O-T/O).

2.2.3 Data ownership and trust

Three research participants raised the issue of reluctance to share, one explaining this as related to the fear of losing control over information (O-T/O).

One research participant raised the issue that people may not even be aware of the existence of particular databases that may be of relevance to their analysis (O-T/O). Another echoed this concern: ‘you can’t ask if you don’t know what to ask for’ (O-P/O).

---

73 IPB cl 49 imposes a statutory ‘duty not to make unauthorised disclosures’; however, it also provides for exceptions in cl 50; see also cls 114 -116. There are also provisions for collaboration agreements in cls 69-71.

74 IPB creates restrictions on use or disclosure of material obtained under warrants etc (cls 48-51); offences of making unauthorised disclosure of communications data (cl 73). It also requires disclosure regarding retained data (cl 82); retention and disclosure of material obtained under various warrants (e.g., cls 112-116; cls 132-135; cl 150; cl 168); examination of material obtained under warrant (cl 151; s170-171). IPB cl 196 also imposes a duty on the Investigatory Powers Commissioner to ‘keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to—(a) the interception of communications, (b) the acquisition or retention of communications data, (c) the acquisition of secondary data or related systems data ... or (d) equipment interference.’
Summary and Implications

Most of the identified barriers to data sharing in the UK were similar to those mentioned in the Australian study. Issues raised in Australia but not the UK include federalism, legal limits on process, different interpretations of legal requirements, compatibility of data formats, handling data volume, reliance on personal relationships, and over-classification. Issues raised in the UK but not Australia include the time taken to negotiate inter-agency agreements, difficulty cross-linking data, technical issues with data extraction and the challenge of knowing what to ask for. While the small sample sizes means differences should not be over-emphasised, it is possible that these can be explained to some extent by Australia’s federal system and the existence of CrimTrac, as well as the possibility that some legal ambiguities are clarified through inter-agency agreements in the UK.

UK participants provided useful details on rules that apply to international data sharing including the focus on location rather than citizenship for categorising data, the third party rule, the risk of compromising operations, and limitations on data sharing on sensitive topics. These rules are likely also applicable to Australia.

2.3 How problems can be overcome

There were a variety of suggestions about how the data access problems raised could be overcome, either through specific interventions or through continuing efforts over time. Interestingly, none of the research participants in operational organisations pointed to the Investigatory Powers Bill as a means of overcoming problems with data access, although the timing of interviews may have meant that most participants had not read the Bill in detail.

The suggestions are organised (below) into the same categories identified in 2.2.

2.3.1 Legal requirements or privacy issues

The only two research participants who addressed this topic did not have specific suggestions for law reform. Rather, both focussed on how a political environment that would support greater access to data might be facilitated. One suggestion was to change the terminology used, particularly in political contexts, so as to avoid the term ‘data sharing’ and focus more on ‘useful words which describe what we’re trying to do’ (O-T/O). Another suggestion was to have a public explanation from technologists as to ‘what we can and cannot trust’ and the comparative nature of different risks (for example as compared with Facebook use). (O-T/O). A similar suggestion was made in the Australian study (2.3.1D).

2.2.2 Technical issues

One research participant mentioned reduced costs of sharing digital data over time as facilitating greater sharing of data across agencies (O-P/O).

2.3.3 Ownership and trust

Three research participants suggested that things would improve over time through formal and informal arrangements. One of the three indicated that efficiency would follow from frequency and that ‘you have to build up confidence’ by working with another agency (O-T/O). The second participant was more concrete about what needed to be established, pointing to the need for agencies to enter into more data sharing agreements (O-T/O). This research participant linked the likely timing of this to a motivating event (such as riots). The third participant suggested joint mission management as a means of facilitating co-operation between agencies (O-P/O). This could involve a physical centre and a virtual community working together on a common intelligence target:

I don’t expect the three [intelligence] agencies to lose their separate identities which is very good for [practical] recruiting purposes, but in practice it’s a bit like the armed forces where
you still have a navy, an army and an air force, but every operation is now controlled by a joint forces headquarters. Very few operations are single service... [Q: Police inside or outside that?] Mixed. Increasingly inside because of the intelligence support needed in order to give the police... the evidence they need. ... Yes, that kind of joint working, that’s the future. (O-P/O A)

Summary and Implications

There are some common threads between the suggestions from Australian and British research participants, including a desire to change the political environment (and a recognition this was likely linked to external events). The most useful new insight from the UK study is the suggested formal and informal means through which trust can be built between agencies, including a combination of time, data sharing agreements and joint mission management. The suggestions to move terminology away from ‘data sharing’ and to engage in comparative risk assessment are also worth noting.

2.4 Big Data: potentials, limits and risks

2.4.1 What is Big Data?

Table 2-3 provides a list of the main responses from research participants to the question: ‘How would you define Big Data?’ [O15, P3] broken down by the type of organisation they worked in.

Table 2-3: Conception of Big Data by Type of Organisation (n=14)

<table>
<thead>
<tr>
<th></th>
<th>Operational (5)</th>
<th>Policy (9)</th>
<th>TOTAL (14)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume</td>
<td>3</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>Analytic/ prediction/ unlocking hidden results</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Aggregated/ integrated data</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Beyond human &amp; established technology</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Variety</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Automated decision-making</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Velocity</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Veracity</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Completeness</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Non-traditional data sources</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Idea misunderstood or unclear</td>
<td>3</td>
<td>5</td>
<td>8</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant, including in the final row. One research participant (P/P) in a joint interview did not answer this question.

There are similarities with the Australian study, particularly the dominant concepts of volume and analytic capacity. Perhaps because we did not conduct interviews in the UK with technical organisations, the idea of Big Data as a marketing term was not mentioned. There were, however, a large number of sceptical responses (8/13) suggesting that the term was either frequently misunderstood or was inherently unclear. There were some characteristics not mentioned in the Australian study such as completeness (over populations and across individual time line), the link with automated decision-making and the use of non-traditional data sources.

One UK research participant sketched out different categories or types of Big Data they deal with in their work:
There is raw information (or BIG DATA), information (or Big Data), intelligence (or big data) and evidence (just data). Raw information is the whole web, every person’s phone billing, everything. … Intelligence is raw information after it has met the hurdle of relating to a target. Intelligence is when we have gone through that person’s information and identified what the criminal actions are. Evidence is when it is used in court. … To me, all of those elements are big data. Need to put context to it to say exactly what you are talking about. Are you talking about ‘big data’ intelligence or ‘BIG DATA’? We are doing different things on different data. For intelligence, we are trying to make sense of all of it; that isn’t so for raw information. What you do with it and how you use it will be different. The generalistic misuse of the word ‘big data’ irritates me – in what context? (O-T/O A)

Another research participant (P/P), using different language, linked raw information (or ‘BIG DATA’ in the above taxonomy) with Bulk Personal Datasets in the Investigatory Powers Bill, preferring to adopt terminology from legislation rather than the more vague term ‘Big Data’.

**Summary and Implications**

There are no significant differences in the understanding of ‘Big Data’ between UK and Australian research participants. The standard definition, involving the three Vs of volume, velocity and variety also appeared in RUSI’s report (1.36). However, there was much scepticism about the term Big Data among operational and policy participants in the UK; some would prefer the more precise terminologies used in legislation or operations.

### 2.4.2 Capability of Big Data

In order to delve deeper into research participants’ concept of Big Data, we asked the question ‘As far as you know, what is Big Data capable of doing that ‘ordinary data’ can’t?’ [O16, P4]. For the policy group, we also asked a more direct question ‘What do you see are the opportunities or possibilities that Big Data can open up for law enforcement and security intelligence?’ [P8]

There were some differences between the UK and Australian results. For example, confidence in data was not mentioned by UK participants, while UK participants mentioned several capabilities that did not arise in the Australian sample (see the highlighted rows in Table 2-4).

The entry ‘answering specific questions’ related to the way in which bulk personal datasets (e.g. telephone directories) were used in law enforcement:

> Going out into [bulk personal datasets] for us is usually directed. We don’t try to make sense of all of it. We go out there with a specific thing we need in the first place. For example, I have a phone number, who owns it? (O-T/O A)⁷⁵

---

### Table 2-4: Perceived Capability of Big Data by Type of Organisation (n=14)

<table>
<thead>
<tr>
<th></th>
<th>Operational (5)</th>
<th>Policy (9)</th>
<th>TOTAL (14)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved efficiency/ effectiveness</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Analytic capacity</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Richness of data</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Need caution re expectations</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Investigative advantage</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Better government decisions/ services</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Answering specific questions</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Opportunity for discovery of unforeseen insights and categories</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Evidence</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>More data driven decision-making</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Predictive policing</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Identification of targets</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Identify patterns and trends</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Real time insights</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Crowd policing</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Risk assurance</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Don’t know</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Nothing on its own</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant.*

There were also differences in the descriptions of some of the capabilities. One research participant in the UK mentioned that the analytic capability of Big Data for national security may differ markedly from the analytic capability of Big Data in the private sector. According to this research participant, what is important is the ability to filter out information, to ‘get rid of as much of the data as possible to get down to that limited part of it which is likely to contain the information that they’re actually interested in,’ which was described as the opposite of what private companies are interested in doing (O-P/O B).  

Interviews revealed some scepticism about big data and related technologies in the UK, with four participants expressing the need for caution around expectations. The relative advantages of ‘better investment in human intelligence’ (P/P) were mentioned by one participant. Another stated:

> I think the public expects police to prevent what may be unpreventable, and it’s through that lens that we’re looking at the effectiveness [of their] policing (P/P C)

---

76 See filter mechanisms in IPB cls 58-60.
Summary and Implications

There are some interesting observations that can be made about the capabilities attributed to Big Data in the UK. At least in law enforcement, bulk personal datasets (non-specific to intelligence targets, such as telephone records) seem to be used for specific queries only. These are discussed further in sections 3.1.5, 3.2.5, 3.2.8, 3.2.9. Some specific advantages of Big Data – not requiring an advance hypothesis but rather allowing for unforeseen insights, using as evidence, facilitating more data-driven decision-making, identification of targets and identification of patterns and trends – were all raised by UK participants but not in Australia (at least not in those terms). However, scepticism about capabilities was quite strong in the UK, with 4/14 participants making the point that there was a need for caution about expectations.

2.4.3 Use of Big Data in work

To investigate the extent to which Big Data (including Big Data analytics) is currently being used for law enforcement and security intelligence, we relied on three sources of information. First, we asked participants from operational agencies the following question: ‘To what extent are you (or your unit) making use of Big Data tools in your work?’ [O17] Their responses represent the primary source of information about use of Big Data for law enforcement and security intelligence. Note, however, that there could be multiple research participants from some agencies. Secondly, participants in policy organisations were asked the question: ‘To what extent is Big Data currently being used for law enforcement and security intelligence in the UK?’ [P5] Some of the responses were based on direct knowledge, while others were based on secondary sources (see 2.6.7).

Table 2-5: Use of Big Data by Type of Organisation (n=14)

<table>
<thead>
<tr>
<th></th>
<th>Operational (5)</th>
<th>Policy (9)</th>
<th>TOTAL (14)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes (including ‘to some extent’)</td>
<td>3</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>Yes but varies</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Perceived yes</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>No</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Perceived no</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Notes: Frequencies in cells do not represent number of agencies, as there were multiple research participants from some agencies. One participant in a joint interview did not answer this question (P/P).

A variety of examples of use (or perceived use – not all research participants worked directly on the relevant programs) of Big Data were mentioned in the interviews (see Table 2-5 for the distribution of responses). Some of these were more focussed on investigating events that had occurred, others were more focussed on understanding the present or anticipating the future. The categories are only loosely defined; understanding the present is often a basis for setting policies directed to the future and understanding the present can be relevant for investigating the past. Below, the examples are listed in order from those most focussed on the past and investigation of historical events, to those painting a clearer picture of the present, more or less explicitly for future-oriented purposes, to those more focussed on the future.

- Access to bulk personal datasets (see 3.1). For example, ‘I believe [the agencies] make hundreds of thousands of requests for communications data every year’ (P/P)
- A centralised access point for distributed data sets (P/P)
- Tool in development using Big Data to analyse ‘the terabytes of video data that [emerge] from a typical investigation’ (P/P)

• Analysis of mobile phone data to determine who was in particular locations at particular times (P/P)
• ‘A large operation involving a number of people who were moving about in different parts of the country, or in different parts of the world. One could see ... a map. ... So if you had movements of people around the country and ... tracking devices had been put on vehicles, you could work out where they were at any particular time. You could see if they were meeting up.’ (P/P, participant did not explicitly identify this with the term ‘Big Data’)
• Analysis of mobile phone data to identify fraudulent activity that fits a particular pattern (P/P)
• Visualisation of complex crime and population data (aggregated to 10,000) (O-T/O)
• Analysis of open source data, such as the ‘Twitter Firehose’ (‘social media analytics’)\(^{78}\), and large scale surveys (2 P/P, O-T/O)
• Large quantities of data allegedly (inference from Snowden revelations) ‘ingested’ by agencies including web browsing records, phone records, email communications, texts messages and medical information (P/P)\(^{79}\)
• Bulk communications data acquisition. Tempora was described as ‘an interception system that then applies ... pre-chosen selectors to intercepted content, and whitltes that down. Then on the basis of the whittled down content, analysts can make searches ... ’ (P/P)\(^{80}\)
• Government agency identifying correlations (e.g. TripAdvisor and health inspectors, timing of passport applications) to ensure efficient regulation and service delivery (P/P)
• Machine learning for intelligence purposes, with inputs primarily being information about known targets (O-T/O)
• Filtering volumes data to identify targets or suspicious behaviours (O-P/O)
• Predicting violence among gang members (P/P)
• Predictive analysis being done at Cardiff University (with Met Police) on social media (P/P)

Predictive policing using ‘historical arrest data’ was also mentioned but was described as ‘not Big Data necessarily’ (P/P). The view was also expressed by a research participant (P/P) that the intelligence agencies are able to make greater use of data compared to law enforcement agencies due to having less public scrutiny of their powers. Another research participant mentioned that police investigate particular incidents or reports, and ‘don’t usually go around just at will, investigating a lot of people who haven’t [had] any complaint about them. You wouldn’t have the resources to do that ... the data collected was all with a view to targeting suspects.’ (P/P A).

We asked research participants to compare the access to data and analytical tools in the UK (or for operational participants, in their agency) with those of foreign counterparts. Of those participants who had a view on this, all eight (being P/P or O-T/O) placed the UK among the leaders internationally. Comparable countries mentioned include the United States, Russia, China, Israel and some countries in Europe. Two research participants (both P/P) pointed out that their judgment was not only based on technology, but also legal permissiveness. One research participant emphasised both capacity and curiosity (O-T/O).

We also asked participants in the policy group whether they believed the use of Big Data for national security and law enforcement purposes should be expanded. Only one (P/P) research participant believed that it should be expanded, also recognising that public engagement would be required. Two (both P/P) research participants believed that it should not, while four (all P/P) believed that any expansion should be conditional on a case being made, including that it is overall in society’s interests. One research participant (P/P) did not express a view.

Summary and Implications

A significantly higher proportion (11/14) of research participants in the UK compared to Australia (14/38) reported that Big Data was being used (sometimes qualified by reference to extent, variation between agencies, or limited knowledge) in their own (operational) work or for law enforcement and/or security intelligence purposes. This is consistent with the view of all research participants who commented that the UK is internationally a leader on data and analytics for law enforcement and national security. Most of the examples of Big Data use were focussed on investigating past events or understanding the present; only three examples concerned predictive analytics. One research participant’s point that ‘curiosity’ was an important factor in the use of Big Data was also of note.

2.4.4 Current use of data analysis tools

Research participants in operational organisations were asked several questions designed to elicit information about the tools used, including as to what they did with data, their use of data visualisation and data analysis, as well as specifically about techniques and software (off the shelf and custom tools). All five research participants described using some kind of data analysis, with similar types of activities to those coming out of the Australian study. There seems, however, to be greater reliance on traditional statistical analysis in the UK, with some research participants describing statistical inference conducted by their unit.

Table 2-6: Current Use of Data Analysis Tools by those in Operational Organisations (n=5)

<table>
<thead>
<tr>
<th>Number of participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data analysis (in general)</td>
</tr>
<tr>
<td>Data visualisation/Mapping</td>
</tr>
<tr>
<td>Data browsing/ searching/ sorting/ linking/ summarising</td>
</tr>
<tr>
<td>Statistical analysis</td>
</tr>
<tr>
<td>Network analysis</td>
</tr>
<tr>
<td>Predictive/ automated/ machine learning tools</td>
</tr>
<tr>
<td>Not in my unit</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant.

Off the shelf (or sometimes customised off the shelf) software used includes Excel, Tableau, SPSS, R, SAS, Stata. One research participant described how ‘we have built our own capabilities made up of a ‘composite of tools’ to extract data in the first place, to clean the data, to visualise the data better, or present it or analyse it better. The team would code that themselves.’ (O-T/O A).

One research participant, working in government in a policy role, described how one unit is building an API [Application Programming Interface] to allow centralised access to distributed government datasets (P/P B).

Summary and Implications

As in Australia, operational organisations seem to be using a variety of data analysis and data visualisation tools. Many (3/5) UK operational participants reported relying on traditional statistical analysis rather than newer data science techniques.

2.4.5 Barriers/challenges to Using Big Data

To understand the barriers or challenges to the use of Big Data, we asked participants several questions. First of all, we collect responses from participants from the operational group to the
question: ‘What are the most serious issues/problems that may prevent you (or your unit) from making more use of data analytics/Big Data?’ [O13, O18]. This is supplemented by responses to two questions we asked of the policy group: ‘What are the barriers (to the use of Big Data for law enforcement and security intelligence)?’ [P8] and ‘What are the challenges ... of Big Data technology to support law enforcement and enhance national security?’ [P9] Results are set out in Table 2-7.

Table 2-7: Barriers/Challenges to Use of Big Data by Type of Organisation (n=14)

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Operational (5)</th>
<th>Policy (9)</th>
<th>TOTAL (14)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical and other resources</td>
<td>5</td>
<td>4</td>
<td>9</td>
</tr>
<tr>
<td>Legal/privacy issues (including consent requirements, proportionality requirement)</td>
<td>1</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Data format/data quality</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Access to/sharing of data (particularly nominal data)/data silos</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Cultural issues</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>User confidence, curiosity, literacy</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Public acceptance/trust</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Understanding of user needs</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant. Not all research participants responded to this question.*

In the UK, technical and other resource limits was the most frequently nominated challenge. Resource limits included working with archaic systems, systems that do not talk to each other, databases not designed for data extraction, as well as access to funding, software, processing power and sufficient (technically trained) human resources.

The second most common response was legal and privacy barriers. According to one research participant, the main legal obstacle to greater use of Big Data techniques is that ‘the law requires a strict application of necessity and proportionality tests’ (O-P/O). One research participant believed that consent was crucial in determining whether the use of data was appropriate (P/P). Another research participant (P/P) also pointed more generally to the need to consider negative privacy impacts and use data for the purpose for which it was collected.

The four participants who mentioned challenges in relation to data raised diverse, quite specific, issues ranging from technical to cultural:

- The possibility of getting lost in a ‘huge sea of far too much information’ (P/P)
- The difficulty extracting data from some databases (O-T/O),
- The difficulty of analysing data in unstructured formats (O-T/O),
- The fact that law enforcement officers sometimes do ‘paper recording’ and ‘general poor collection of data’ which was described as an aspect of ‘police culture around data storage, and data entry’ as well as poor knowledge of basic data tools such as Excel and Access (O-T/O).
- The poor quality of and potential for systemic bias in social media data (O-T/O)
- The fact that data may be biased ‘because you’ve always arrested more young black kids than young white kids’ (P/P)
One research participant observed the difficulties for UK agencies obtaining access to data held by private corporations overseas, such as Facebook and Google (P/P). The same issue was raised in the Australian study.81

Cultural issues included ‘getting operational members of staff and policymakers to be hungry and curious about this data’ (P/P)

Some of the issues identified in our study align with ‘key challenges’ for security and intelligence agencies identified by RUSI (3.43–3.59), including access to technical resources and expertise. RUSI also referred to additional challenges including the large number of relevant data custodians (e.g. Internet suppliers) and encryption.

Summary and Implications

Research participants in the UK and Australia reported similar types of barriers to the use of Big Data; for example, both groups operated under resource constraints. UK participants were much more likely than Australian ones (9/14 vs 8/37) to focus on technical and resource issues. Although Australian participants nominated legal and privacy barriers most frequently, the proportion of responses was similar to that in the UK sample. Legal issues that were identified in this study reflected the nature of the UK regime, including the requirement for necessity and proportionality.82 UK participants were more aware than their Australian counterparts that some of the data collected may be incomplete or biased. This concern was not raised by the Australian participants.

Technical and legal barriers are both real. Continuing technical barriers can subvert the intentions of legislators; legal barriers cannot be ignored by technology designers or dismissed as an obstacle to be overcome. Further, those using data science techniques need to bear in mind biases and limitations of the underlying data, which may require an understanding of cultural factors influencing its collection.

2.4.6 Risks of using Big Data

To examine participants’ perception of the risks of using Big Data, we asked a similar question of each group: ‘What are the risks of using Big Data for law enforcement or security intelligence?’ [O19 and P9].

---

81 The IPB deals with this issue indirectly through warrant implementation regime in cl 35 and cl 36 (duty to assist with implementation); police collaboration agreements (cls 71 and 76); equipment interference warrants (cls 91 and 109–111).
82 See 3.2.
Table 2-8: Risks of Using Big Data by Organisation of Research Participant (n=14)

<table>
<thead>
<tr>
<th>Risks</th>
<th>Operational (5)</th>
<th>Policy (9)</th>
<th>TOTAL (14)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misuse of data</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Privacy</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Misplaced trust in technology/assumptions behind analytics</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Proliferation challenges*</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Data security / honeypot risk*</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Data quality/integrity</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Discrimination</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Freedom of speech and related impacts</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Political and reputational risks</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Public perceptions</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Usefulness as evidence</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Misdirected resources</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant. Not all research participants responded to this question.

\*This refers to the risk that an authoritarian government (either a foreign government or a future UK government) may apply similar rules or tools to those being proposed currently in the UK.

One research participant (O-T/O) expressed the view that there are manageable risks ‘as long as you are using big data within the proper legalities, policies and processes’.

The dangers of **internal misuse of data** were important for five research participants, for example:

[I]t’s critically important that one sees that systems are in place to prevent a rogue getting in or operating within, because obviously the powers of investigation into the data I’m talking about, this Bulk Personal Data, are very great. If you get a rogue in the place and the power to use their systems for their own purposes, that’s very serious indeed — so that’s the risk that you have to guard against. (P/P A)

[W]e’ve seen journalist sources being spied on — even lawyer client communications in a torture case that was being brought against the UK Government. So having that data available presents a real risk too. (P/P B)

We know in the US there’s been a number of people sacked for LOVEINT. So abusing the systems to find that information about people, and you can put some processes in place for that, but it becomes harder to do when you look at data [that] becomes more abstract. I can say well I’m looking for people who have done this thing and that thing. I happen to know that includes the person I’m interested in. (P/P C)

Risks around **misplaced trust in technology** largely involve the risks of reliance on automated systems, particularly where there was a potential for punitive outcomes (such as no fly lists) (P/P). One participant mentioned the importance of having a human oversee automated decision-makers so that ‘if [the fact that] you’re being flagged is totally erroneous, then you would hope that that investigation would stop there’ before, for example, automated malware distribution systems were released (P/P D). On a similar note, another research participant was concerned that ‘because it can be churned quickly with machine learning and the rest, you can make wrong decisions because you don’t put the time and effort in to investigate whether it’s true or not.’ (O-T/O E)

---

**Data quality and integrity** and thus confidence in inferences may be more or less important in different contexts (criminal prosecution versus security intelligence for example) (O-P/O).

Participants mentioned the importance of analysts’ understanding the limits of analysis due to data integrity (O-T/O), particularly in the case of social media.

Two research participants raised risks around **freedom of speech**, particularly on the Internet:

> The lack of ability to be anonymous, ... I think that that really will, in the long-term, impede development of thinking and creative endeavours and progressive movements and social change in ways that we can’t really measure. I think long term, we will come to regret the fact that the internet’s become such a sanitised space in some regards. (P/P F)

One research participant raised the issue of **misdirected resources**:

> Actually that seems to be a fairly pervasive thing that [law enforcement and security intelligence agencies’] problem is a lack of people and resources to deal with the data there already is. [Gives example of case where information about 2345 people viewing child abuse images was not acted upon for at least 14 months]. So I’ve always been, particularly since I found out about that, slightly alarmed at these calls we must have more powers to tackle paedophiles. It seems like actually the power that was needed then, was the power to look at an email and get on with it. (P/P G)

**Summary and Implications**

Most of the risks identified in the Australian study were also mentioned in the UK study. The exception was ‘overload’ (which was mentioned by four Australian participants), but while that was not recognised as a risk in the UK, constraints on human resources were mentioned as a barrier. In the UK sample, data issues were mentioned more often than legal and privacy issues. Further, some new issues were raised, in particular the risk of a negative impact on freedom of speech, risk of proliferation, the possibility that the outputs would not be useable as evidence in court, and the potential for resources to be misdirected. Some differences in identified risks could be due to the European human rights framework within which the UK operates, and the history of colonialism which gives the UK continuing international influence. The potentially limited use of the outputs of data analytics as evidence in court exists in both countries, but this type of use is not the primary objective in either jurisdiction (see 2.1.5). Similarly, balancing resourcing demands is likely relevant in both jurisdictions. We cannot draw conclusions from risks omitted in UK interviews due to small sample size.

### 2.4.7 Who is exposed to these risks?

Where it was not clear from research participants’ identification of risks, we asked research participants who they felt was exposed to the risks they had identified. The results are shown in Table 2-9.

**Table 2-9: Who is exposed to risks of Big Data by Organisation of Participant (n=14)**

<table>
<thead>
<tr>
<th>People at risk</th>
<th>Operational (5)</th>
<th>Policy (9)</th>
<th>TOTAL (14)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone/the community/citizens as individuals</td>
<td>0</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Government decision-making</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Minorities/marginal people/young people/people of certain SES/refugees</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>People identified in data/lone citizens</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant. Not everyone responded to this question.

There was a clear division in responses between the operational and policy groups. Those in the operational group focussed on risks for government decision-making, whereas those in the policy
group described the exposed groups as ‘everyone’ or ‘citizens’, as marginal groups and/or as individuals identified in data through analytics as potential threats. This cannot be compared to the Australian study because we did not collect this information from the operational group for that study. However, overall, the categories identified were similar.

One difference was that, in the UK study, there was concern about government as such, in particular around poor decision-making, but no expressed concern about government workers (as there was in Australia). Similarly, no research participants mentioned agency personnel, informants or academics/researchers. While there was no mention of people of interest to law enforcement and security agencies, there was mention of people identified as potential targets through analytics, which links back to the risk of poor decision-making.

**Summary and Implications**

Respondents in the UK and Australia were equally concerned about the broad risk to the community and the risk to disadvantaged groups. They were also concerned about the potential for poor quality decisions if data analytics was done badly and the impact on government of mistakes.

### 2.4.8 Management of Big Data risks

For the policy group, we also asked ‘How should these risks be managed?’ [P9]. Some in the operational group gave unprompted suggestions as well, and these have been included. Table 2-10 provides a cross-tabulation of the risks against suggested approaches to the mitigation of these risks. A number of suggested approaches are applicable to several types of risks.

Responses in the UK overwhelmingly focussed on appropriate regulation and sanctions (including international law), a range of educational initiatives and better public engagement and government transparency. While these strategies were also nominated by Australian participants, the emphasis in the UK study was quite different.

In relation to **appropriate regulation**, suggestions included strong sanctions for data misuse (P/P) and a human rights based framework (P/P). There was specific mention of the need for European or international regulatory mechanisms, in addition to national mechanisms. Regulation was also perceived as a means of dealing with almost all categories of risk (with the exception of political risks and public perceptions).

**Education** was also perceived to play a role in managing different types of risk. There was a broad spectrum of groups who participants believe could benefit from education. Examples included:

- education of technology designers ‘on the societal impacts of algorithms and Big Data analyses and how to make the technology itself a tool for good...’
- education of those working with data so they appreciate ‘the privacy impact of what they are doing’ (P/P)
- education of operational personnel on ‘statistical analytical evidence driven’ approaches (P/P), as well as limitations in the data (O-T/O). A better understanding among operational personnel of what data science can do was also seen as useful in promoting the (appropriate) use of data science (P/P).
- education of the public on the data science opportunities (P/P) as well as rights and obligations (P/P), and
- education of policy makers on technical aspects and privacy aspects (P/P, who pointed out that the technical advisory committee under RIPA had never met and a privacy and civil liberties oversight board had been legislated for but not created).
Table 2-10: How Big Data Risks can be Managed (n=14)

<table>
<thead>
<tr>
<th></th>
<th>Data security</th>
<th>Data integrity</th>
<th>Misuse of data</th>
<th>Privacy</th>
<th>Misplaced trust in technology</th>
<th>Disinformation</th>
<th>Freedom of speech</th>
<th>Political risks</th>
<th>Proliferation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appropriate regulation/sanctions</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Education</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Better public engagement/external transparency</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Limit uses</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>More targeted surveillance</td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk mitigation via design</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controls/oversight</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluation</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Realistic expectations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Long term view</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screening employees</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law reform</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consent</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: Multiple responses can be coded for each research participant. Not everyone responded to this question. Not all risks identified in Table 2-8 are included here.

Strategies around public engagement and transparency were mentioned by six research participants, sometimes in relation to multiple risks but most often in relation to privacy. There were various components in this, ranging from government being open and transparent about benefits and risks (P/P) and the need to be more open about justification for particular operational capabilities and engage with the public in an ‘evidence driven debate about the use of big data …’ (P/P), to various types of deliberative public engagement. This included mention of deliberative workshops held with the public over two days involving responses to scenarios and testing of a data ethics framework (P/P) and early engagement (by government and technology companies) with relevant NGOs concerned about particular ethical issues in order to facilitate mutually satisfactory problem solving (P/P). Overwhelmingly, suggestions focussed on engagement with the public as well as ensuring that they were appropriately informed.

While other suggestions were not made as frequently, there were some particular noteworthy suggestions in relation to oversight. One research participant described how they had implemented a data ethics framework, including a checklist of questions encouraging people to explore issues

---

such as public benefit and risk (P/P). This was said to be of interest to ‘lots of countries’ (P/P).

Another research participant explained the kind of internal oversight required (in addition to external oversight) to prevent misuse of data:

They already have systems in place and the starting point is to make sure you don’t employ people that you can’t trust. The second thing is you must make sure that nobody can operate on their own. The third way is to make sure you with modern era computers, you are able to make sure that if somebody uses a system which they shouldn’t be using bells will ring — I’m talking figuratively — in the right places. (P/P)

Some responses were generally negative towards the use of Big Data or large scale data sharing. These are not included in the table as they are not about managing risks of an assumed activity, but rather not taking part in that activity (at least to the same extent). One research participant wanted to limit the uses of personal data to situations where there was consent for such use and the data was used for beneficial purposes such as service delivery in a non-discriminatory way (P/P). Overall, this research participant preferred to limit the use of Big Data as a means of solving problems.

Another research participant described how data exchange was already minimised so the minimum data was provided as was necessary for the program ‘which means less collateral intrusion’ (P/P). For automated systems, this research participant suggested that they should include a warning where a system is asked for more data than seems likely to be needed.

Other suggested solutions for managing risks generally rather than particular risks (and thus not included in the above table) were:

- having proper evaluation of Big Data initiatives in order to facilitate learning (P/P), and
- bringing researchers, policy makers, industry and investors together to find solutions to problems (P/P)

### Summary and Implications

The main differences in relation to the management of Big Data risks between the Australian and the UK participants were the following: the UK sample had a greater focus on international law and human rights frameworks in the context of regulation, a broader understanding of the different groups that might benefit from education or training, and more emphasis on the idea of public and multi-stakeholder engagement (two way rather than one way communication) combined with greater government transparency. Existing UK initiatives on a data ethics framework, evaluation processes and minimisation of data sharing are also worth noting, as is the suggestion for system warnings when data requests are excessive. The impact of the IPB filtering mechanism on these developments is discussed in sections 3.2.4 and 3.6.2.

### 2.5 Regulation

In this section, we analyse the responses of research participants to questions relating to how Big Data as a category, or the access, disclosure, use and destruction of data more specifically, is or ought to be regulated. Different questions addressed different aspects of regulation, which are dealt with as follows:

2.5.1 Description of laws, regulations, and internal guidelines

2.5.2 Description of accountability, transparency and oversight ‘mechanisms’ other than those embodied as above

---

85 Some considerations from the data ethics framework are codified in the IPB though at a very high level: see cl 196 (5) ‘In exercising functions under this Act, a Judicial Commissioner must not act in a way which the Commissioner considers to be contrary to the public interest’; cl 198 (1) ‘The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person of which the Commissioner is aware if the Commissioner considers that (a) the error is a serious error, and (b) it is in the public interest for the person to be informed of the error.’
2.5.3 Views on the appropriateness and effectiveness of 2.5.1 and 2.5.2
2.5.4 Identification of specific shortcomings of 2.5.1 and 2.5.2, and proposals for reform
2.5.5 The extent to which technical tools are, could or should facilitate ‘regulation by design’

2.5.1 Laws, regulations, and internal guidelines

As in Australia, asking research participants to identify laws, regulations and procedures governing the use of data by law enforcement and security agencies was not for the purpose of creating a comprehensive list of such laws. Rather the goal was to describe participants’ understanding and perception of how the use of data is regulated. The results are shown in Table 2-11.

There were many similarities between the UK and Australian studies in the types of legislation that research participants mentioned. For example, the relevant privacy law (such as the Data Protection Act) was often mentioned only in relation to its being inapplicable due to agency-specific or purpose-specific exceptions. There does, however, appear to be greater cross-sectoral awareness of important categories of regulation in the UK compared to Australia, possibly the result of recent legislative and related activity. However, the Telecommunications Act which was perceived by two research participants as a means of bypassing oversight under the then governing statutory regime, was not mentioned by participants within in the government or independent sectors.

Table 2-11: Legislation and regulatory material identified by research participants according to (1) organisation sector, and (2) type of organisation (n=14)

<table>
<thead>
<tr>
<th>Category</th>
<th>Research/ NGO (5)</th>
<th>Independent (3)</th>
<th>Government (6)</th>
<th>Policy (9)</th>
<th>Operational (5)</th>
<th>Total (14)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection Act or European data protection</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>9</td>
</tr>
<tr>
<td>RIPA/DRIPA and associated Codes of Practice</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Agency specific or purpose-specific legislation (e.g. law enforcement/national security/counterterrorism)</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Internal guidelines&lt;sup&gt;1&lt;/sup&gt;</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>European instruments</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Telecommunications Act</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Memoranda of understanding</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Dataset specific legislation</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Freedom of Information Act</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Human Rights Act (and ECHR)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>National security directions</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Data ethics framework</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Don’t know/ unsure</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

* Multiple responses can be coded for each research participant, including in the final row. In some cases, the legislation was not named but described and classified by the authors.

<sup>1</sup> Includes manuals, protocols, guidelines, codes of practice

Across the legislative specifics, the requirement for proportionality (see 3.2) was mentioned by 8/14 research participants. It came up in a variety of contexts, often in this question but sometimes in
responses to the scenario (2.6.3 below). It was sometimes discussed in the context of related principles, such as the principle of necessity. For example:

Everything we do has to be proportionate (O-T/O A)

[Agency] is bound by the law and the law requires a strict application of necessity and proportionality tests. (O-P/O B)

There has to be evidence of necessity. There has to be proportionality. There has to be accountability. (P/P C)

You can use [bulk personal datasets] in what’s called a proportionate manner: that is to say that the invasion of privacy which there will be is protected as far as possible and is justified by the necessity to use the system. ... They will have to go to somebody who does have access i.e. authorisation and they will have to justify to that officer, who will have to justify to himself or herself that it’s necessary to do this and that it is proportionate to do it. (P/P D)

Proportionality requires us to understand what is the harm that we’re doing. (P/P E)

The wider the authorisation, the more carefully one looked at what the justification for it was... The general principle of proportionality is that you only use extreme measures to deal with extreme situations. So you don’t have to start with extreme measures. ... If you’re looking at the reasonableness of an authority to intercept in an imminent situation, you would take the imminence into account, the seriousness of the threat, if this information wasn’t obtained. (P/P F)

It would seem that, generally speaking, agencies cannot access bulk personal data except on a case-by-case basis, although that may amount to a large number of requests (P/P). The IPB regime in relation to this is described in section 3.1.5 –3.2.2.

One research participant described the government’s data ethics framework. More detail on this is at 3.2.3 and at <https://data.blog.gov.uk/2015/12/08/data-science-ethics/>.

We also asked all but two research participants (both P/P) whether any of these laws regulated Big Data, or analytic techniques, as such. Relevant elements of the IPB are discussed in section 3.1.5. Most research participants (7/12) answered in the negative; two of these noted that the general proportionality principle would apply (O-T/O, O-P/O). Those who answered positively gave the following examples:

- Rules through which people can establish their identity online for the Verify system (P/P)
- Right of explanation and challenge in the Data Protection Act, where an automated decision is made about a person (never happens in practice) (P/P)
- Requirement for ‘fair’ processing (O-T/O) or rules that apply to processing of personal data (P/P)

**Summary and Implications**

Research participants in the UK identified a wide range of legislation and regulatory instruments governing the use of data. Differences between the research/NGO sector and the government sector were limited to the least mentioned categories: European human rights instruments, the *Telecommunications Act* and national security directions (research/NGO only) and memoranda of understanding, dataset specific legislation, ethical codes and information management requirements (government sector only).

As in Australia, internal guidelines are often a primary reference point within operational agencies.
Also similar to Australia, most existing UK laws focus on data collection and access, not data analysis. There were some examples given where the law did potentially restrict data analysis, including the general proportionality requirement, the right to challenge automated decisions and a requirement for ‘fair’ processing. There are further provisions in the IPB.

Perhaps most significant is the fact that the requirement for proportionality was mentioned very frequently, cutting across particular identified legislation. The principle would seem to be very familiar within the UK context across a broad range of roles and organisations. This may be due to the fact that the concepts of necessity and proportionality are embedded ‘in the practices and training materials of all public authorities who apply [RIPA]’ (Anderson 5.18). Conversely, the principle of proportionality was only mentioned in two Australian interviews.

2.5.2 Accountability, transparency and oversight mechanisms

We asked all research participants, not only about formal laws and guidelines, but also about accountability and oversight mechanisms governing the use of data. (See 3.6 for our summary of the legal position.) A range of mechanisms were identified, falling into similar categories to those in Australia.

External mechanisms identified in the UK study included:

- Parliamentary oversight (although it was also noted that not everything need be reported to Parliament)
- Oversight by Commissioners, particularly the Information Commissioner
- Oversight by the IPT
- Warrant requirements (also in the context of ‘double lock’ under the *Investigatory Powers Bill*)
- External audits
- Courts (in their willingness to receive evidence)
- Corruption investigations

Internal mechanisms identified in the UK study included:

- Agency processes
- Internal audits and automatically generated audit trails
- Security audits
- Data compliance officers; internal legal departments

Ethical codes were also mentioned as an important mechanism.

Summary and Implications

As will be explained in 3.6, the UK oversight regime differs from the Australian regime. In particular, under the current law, there are separate Commissioners and Tribunals that split the role played in Australia by organisations such as the Inspector-General of Intelligence and Security (IGIS). This regime will be changed under the IPB (see 3.6). However, as in Australia, the UK relies on both independent/external and internal oversight mechanisms.

2.5.3 Appropriateness and Effectiveness

In the UK study, all research participants were asked ‘In your view, are these laws, regulations, procedures, guidelines (including accountability and oversight mechanisms) appropriate and effective?’ [O20, P10c]. Their responses are captured in Table 2-12. As was the case in Australia, there is a clear division between those in the research/NGO sectors who were sometimes critical

---

86 The *Data Protection Act 1998* (UK) is discussed in more detail in 3.1.2 and 3.4.1.

87 *IPB* cls 134, 151, 170, 190 and 191.
(particularly about oversight) and those in the government sector who were generally uncritical, or focussed on restrictiveness.

Table 2-12: Evaluation of appropriateness and effectiveness of laws, regulation and oversight by research participants by (1) sector of organisation and (2) type of organisation (n=14)

<table>
<thead>
<tr>
<th>Category</th>
<th>Research/NGO (5)</th>
<th>Independent (3)</th>
<th>Government (6)</th>
<th>Policy (9)</th>
<th>Operational (5)</th>
<th>Total (14)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive comments</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Negative comments</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Generally positive with other comment or critique</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Positive or neutral about oversight; negative about restrictiveness, red tape or reduced capacity</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

In the government sector, responses were generally positive. One research participant who was positive about appropriateness (O-T/O) mentioned that effectiveness was dependent on compliance. There was also concern about access to data:

[T]hey think that somehow by having a name is a violation of confidentiality. I do not agree. A name to me is the only way of tracking everything beyond the name. The name is irrelevant, but unless you have that name to track you can’t do it. (O-T/O A)

One research participant who had worked in government expressed the view that the Investigatory Powers Bill regime would be appropriate and effective, would provide improved clarity and was ‘pretty comprehensive’, noting as well that oversight and control regimes were tighter but that the powers themselves were almost identical (O-P/O). Another research participant also commented that the impact of the changes affected were ‘minor’ due to the policies and processes already in place (O-T/O). The others did not comment.

Those working in independent agencies were generally positive, although one (P/P B) mentioned that the legislation was sometimes, like a lot of legislation, unclear. This research participant also pointed out limits to what legislation and judicial review could achieve, noting that, ultimately, ‘the most important thing about all of this [judicial review process] is that it operates, to a certain degree, on trust.’ Even with extensive powers, suggested this research participant, those hearing complaints had to trust ‘in cooperation with the bodies that were complained about.’

The five research participants from the research/NGO sector were uniformly negative about the protective aspects of the current legal regime, although for varied reasons, and (where they commented) had different reactions to changes in the new Investigatory Powers Bill:

- Lack of funding for commissioners who oversee the agencies (2 P/P)
- Lack of clarity about existing powers and oversight, some of which was said to be carried over to the new Investigatory Powers Bill (P/P)
- Lack of regulation and guidelines in areas such as open source intelligence (e.g. Twitter ‘firehose’) (P/P)
- Weak accountability mechanisms, in particular no appeal from Investigatory Powers Tribunal (P/P)
- Legal regime too permissive, particularly for intelligence agencies (2 P/P)
- Reliance on the Telecommunications Act for interception and Intelligence Services Act for data collection, which allegedly have fewer safeguards (P/P)

---

88 See also 3.6.1.
• Codes of Practice are ‘woefully inadequate’ and ineffective (P/P) or take too long to be passed (historically) or introduced (currently) (P/P).

• RIPA is ‘an atrocious piece of legislation, [i]t’s written in very, very unclear ways’ and is out of date (P/P). For this participant, while the Investigatory Powers Bill effects an improvement (‘[i]t is better to have ... bad law ... than hidden’, it is more clear), there are still problems such as the ability to vary warrants after approval (P/P) and it is ‘massively intrusive’ and creates additional powers, in particular the collection of internet connection records and bulk equipment interference. ‘Not [appropriate and effective] at the moment, but I think what the government is doing now to update the laws with the Investigatory Powers Bill is going a very long way.’ (P/P)

General positive comments about the Investigatory Powers Bill by participants in the policy group included:

• Increased transparency (3 P/P)
• Increased clarity (3 P/P)
• Having one body oversee all warrants and the intelligence agencies (P/P)
• More up to date (P/P)

Four research participants in the policy group, however, expressed the view that the new Bill would not make a difference to agency practice and thus represented a missed opportunity for better protections:

My suspicion, and I think it’s probably right, is that they’re doing everything in this Bill already anyway. ... [T]his is just ... their attempt to enshrine them into law. (P/P C)

I don’t believe that the new system will provide any greater protection. It may provide greater public reassurance, but also of course there is the added bureaucracy which means more staff in intelligence services doing these processes. (P/P D)

... international data sharing will remain fairly uncontrolled. ... [In response to a different question] If this is our post-Snowden debate, it’s a very sad one because we’re saying, we found out all this shocking and controversial information on how our typical expectations of not being searched without suspicion and so on have been tracked. The kinds of things that we said before we had documentary evidence from Snowden, would be unacceptable and only typical of authoritarian countries. We’d never do it in our own country. Now we know that we are and if our response to that is to say, well let’s just put it into law, that’s not a very good one. ... It’s basically entrenching into law some extraordinary practices that are not human rights compliant. (P/P E)

So we need new legislation because RIPA is so out of date, section 94 of [the] Telecommunications Act is so bad, we definitely need new legislation. But to quote [the] Intelligence Security Committee, it’s a missed opportunity. To quote David Anderson, independent reviewer of terrorism legislation, it’s a work in progress. It leaves ... [a] lot of powers yet still need to be considered, I can’t remember his exact phraseology, I tweaked it. ... This is now a draft in a form that could be considered by a bill committee [as] a draft, it hasn’t progressed beyond that stage. It needs to. (P/P F)
Summary and Implications

Similar to the findings in Australia, UK research participants working in government were generally more positive about laws, regulation and oversight than those in the research/NGO sectors. There is a greater overlap in relevant laws identified between different categories of research participants in the UK compared to Australia. The explanation for differences in views in the UK thus likely rests heavily on differences in values (see 2.6 below) and challenges of trying to perform particular functions with limited access to data. Opinions about the appropriateness and effectiveness of the Investigatory Powers Bill (earlier version) were mixed. The Bill seems to have resolved some (not all) participants’ concerns about transparency, clarity, simplicity, comprehensiveness and currency of existing laws. However, those concerned that the current legal regime was too permissive retained the same concern about the Bill.

2.5.4 Perceived shortcomings in law and regulation and proposals for reform

We asked all research participants what shortcomings they perceived in law and regulation concerning the use of data and analytics for law enforcement and national security and whether they had any suggestions for reform. We also asked what other regulatory and management strategies were required. Responses are complicated to some extent by timing. During the interview period, the revised Investigatory Powers Bill was brought before Parliament. Therefore some reform suggestions from earlier in the interview period may be reflected in the revised Bill. A fuller explanation of the revised Bill is in Chapters 1 and 3. Further, research participants had varied understandings of the existing and proposed legal regime and existing agency practice. In this section, we do not evaluate the proposals for reform.

In the UK, a number of research participants focussed their discussion of shortcomings and reform proposals on broadening or narrowing the powers granted to the agencies and/or enhancing privacy protections. These included:

- Two participants (both O-T/O) in the operational group suggested that there should be access to more data or to more relevant, and proportionately accessible, data. One research participant from the NGO/research sector agreed that there should be a greater ability for government departments to share data for evidence-based policy making (P/P).
- On the other hand, three research participants from the policy group expressed the view that surveillance and/or data retention should be scaled back or made more targeted, so that government could not collect everyone’s data. This view was explained as consistent with the position that the privacy breach occurs when data is collected, not when it is accessed by a human or used, and the importance of consent.

Building better mechanisms for oversight, accountability and ethical evaluation. A number of participants in the policy group had a range of suggestions to improve oversight and accountability and encourage internal ethical evaluation. Some of these are dealt within the IPB (see Chapter 3). Suggestions included:

- Employing the data ethics framework, having ethics committees or an ethical council, creating technical standards and self-checking algorithms (P/P).
- Safeguards around processing of data as well as existing safeguards for collection, retention and human examination (P/P).
- People authorising access to data should be independent of the investigation, even if working in the same organisation. For small organisations, this may require authorisations from a different entity (P/P).

---

• Need for audit trails (P/P).\(^{91}\)
• There should be a proper independent oversight body, with technical as well as legal skills (P/P). This also needs to be properly staffed and funded (P/P).\(^{92}\)
• There should be limits on the circumstances in which warrants can be amended without re-authorisation (P/P).
• There is a general need for stronger data protection laws which restrict ‘bulk hacking’ and mandate more targeted approaches (P/P).\(^{93}\)
• Computers should not be able to make decisions ‘that have real bearings on people’s liberty and security’ (P/P).

It is worth noting here that there was also opposition to the idea of more regulation lest it ‘prevent the agencies actually doing the job which they are there to do (P/P) ... we hope that they do in order to protect us (P/P)’ (joint interview).

There were also a variety of specific comments on aspects of the new Bill, such as the double lock regime (requiring that a minister of state and judicial commissioners authorise interception warrants), which will be discussed in 3.2.1. This proposal generated positive and negative responses, as well as suggestions for changes:

[D]epending on the extent to which independent commissioners are appointed and the extent to which they are independently able to do their job, then we may see some ... greater regulation of the use [or] acquisition of data. Some more accountability around that process. But that will depend on that function, I think. (P/P A)

[I]s it right that a judge should be able to make that sort of decision? ... I think it is a very difficult question on which I wouldn’t express a view, but I can see there are two points of view about this. (P/P B)

... to provide protection to the public in my view it isn’t strictly necessary. ... I would actually say ... there’s a slight danger that it’s less effective. The reason why I say that is that at the moment what the agencies have to do is ... get authorisations from ministers or get internal authorisations if it’s collecting data or whatever it is. They know that in the next six months somebody ... is going to come and look to see whether what they did was lawful, so they watch over their shoulder to make certain that it is. If you introduce a system under which you say to get your authorisations you’re going to have to go to a minister and a judge, ... there’s a temptation to push the boundaries, because if you get the authorisation by the judge, fine. (P/P C)

There would at least be the involvement of judges in warrants, however it would be a rubber stamp. So it’s basically - it’s a fairly impotent check. ... We would have proper judicial authorisation - one stage, an independent judge. ... A judge who can do a merits based review. (P/P D)

I think the introduction of any sort of judicial process is better than no judicial process [but] doesn’t go far enough. (P/P E)\(^{94}\)

As was the case in Australia, some (4) research participants (O-T/O, 3 P/P) commented on the need to keep the relevant laws up to date or draft them so that they can accommodate new technologies and data types.\(^{95}\) For example:

\(^{91}\) See IPB cl 196
\(^{92}\) The IPB cl 194 will establish the Investigatory Powers Commissioner and other Judicial Commissioners.
\(^{93}\) See section 3.2.7.
These laws were written 20 years ago before machine learning and Big Data really existed. (P/P, noting however that ‘I think it’s kind of fine and it gives good coverage’).

The law doesn’t fit and cover the reality that we’re in today. Therefore, it needs to be addressed through new legislation. That’s what they’re trying to do. (P/P F)

At the moment, they still … define ‘examine’ as human reading, which I think is massively out of date and they know it. Because actually, examining can be done in a far more sophisticated and scaled way by machines which, in practice, is of course what happens (P/P G)\(^96\)

The need for greater clarity and/or consistency of rules (see 3.3) was mentioned by three research participants.\(^97\) For example:

- I think the biggest shortcoming is that it’s … really difficult to understand. I still don’t get it all and I’ve been working on this for two years. (P/P H)
- I just don’t think they’re [the current laws] consistent and everybody seems to have the wrong reading, which means then you … spend an extraordinary amount of time dealing with stupidity. (O-T/O I)
- It’s hard to understand. I’m not sure that the intent is always clearly defined. So there’ll be highfalutin’ words about your responsibilities but not what the intent of use of information is there for. … and we all, because we are risk averse, trying to use the words that are put down there as a reason not to do something, as opposed to looking for a reason to do it for the public good. (O-T/O J)

The importance of having a single source of legislative power (with oversight), rather than alternative regimes without oversight.\(^98\)

Their answer is so that safeguards are available if the agencies want to use them, basically, which is beyond farcical. … [T]he agencies will be able to choose. Do I want to collect a data set under the Investigatory Powers Bill and there are safeguards and mechanisms around me doing that? Or do I just want to collect it under the Intelligence Services Act? (P/P K)

[Telecommunications Act s 94] says that, the secretary of state may give a direction to any telecommunications provider to do anything, directions of a general nature, in the interests of national security or relations with another country. Now that’s quite a powerful instruction. You can tell them to do absolutely anything, not just national security, but if another country wants you to it. Now because it’s so powerful, it is written in to the legislation that it has to be reported to parliament any time it’s used. However, there’s an exception, which is that it cannot be reported and indeed must stay completely secret, if - to report it would either breach national security or relations with another country or commercial confidentiality. With the result that the use of the power was never formally reported to parliament, only one use of it has ever been avowed. Which was collecting everybody’s mobile phone information, which was only relatively recently avowed from the home secretary announced this. … So eventually the prime minister did ask the communications commissioner I think it was, to have a look at it. His report said that he had been asked to look at it, but there were two problems. (1) Because it’s any secretary of state can give these orders and there was no central register of them. He had no idea whether he had even seen all of them. (2) Even if he had any comments to make about them, the law made it illegal for him to reveal their existence what he thought of them. … So that [has] to

\(^{96}\) See further discussion at 3.4.3.


\(^{98}\) This is supported by GCHQ (Anderson Report [10.40(b)]) and civil society organisations (Anderson Report [12.21]-[12.23])
change, but there is a natural security direction which are pretty similarly worded, but not quite as bad (P/P L)\textsuperscript{99}

**Comprehensiveness** One research participant pointed out that the new legal regime should be comprehensive and thus include international data sharing (P/P).\textsuperscript{100}

**Penalties:** One research participant (P/P) suggested that sanctions and penalties for theft or misuse of data ought to be stronger.\textsuperscript{101}

**Incorporate privacy into the Investigatory Powers Bill.** This aligned with the Intelligence Security Committee’s recommendation on the draft Bill (see 1.3). P/P.

**Evidence.** Two research participants (both P/P) believed that intercept evidence should be able to be presented in court.\textsuperscript{102}

**Definition of personal data.** One research participant believed the definition of personal data should be changed so that it can include data about more than one person:

> ... our definition for sensitive, for personal data, is that it has to be data which could be identifiable to one person, given either information that you have, or stuff you are reasonably likely to get. But the big problem is it applies to a single person. So data which applies to you or your husband, is not personal data. ... It’s not personal data, unless data I could have or reasonably get, would allow me to work out which one of you it was. That’s a very strange way of doing it. So somebody living alone, knowing when they use electricity would be personal data. If it’s two people knowing when they use electricity it’s not personal data. Though it’s not obvious starting from anywhere else that there’s such a clear distinction. I mean one of them say that knowing when people in that hall of residence over there of the 200 people, when electricity is used, is not personal, I think we’d all be happy with that. But it’s odd that the line is set at one. (P/P M)\textsuperscript{103}

**Protections for people outside the UK.** One research participant believed that there was a need for the UK to recognise the human rights and privacy rights of people outside its borders.\textsuperscript{104}

Why should Britain have respect for privacy of people who are standing on these shores more so than people standing outside them? (P/P N)

**Opposition to data retention.** As was the case in Australia, two research participants (both P/P) expressed opposition to the data retention regime on privacy/human rights grounds as well as European law.\textsuperscript{105}

Some research participants focussed not only on the substance of the law but also the **conditions under which decisions about law ought to be made:**

- The need for a discussion about what powers the agencies ought to have based on evidence of privacy risks and security benefits (P/P)
- The need for agencies to make operational cases for the powers they are seeking (P/P)

\textsuperscript{99}This is discussed in 3.1.3.


\textsuperscript{103}See IPB Part 7, ‘Bulk Personal Dataset Warrants’.

\textsuperscript{104}See 3.2.1

Summary and Implications

Research participants raised a variety of specific and general proposals for reform. Some of these may not be appropriate and others may be based on limited knowledge of the regulatory regime or the participant’s limited viewpoint. It is not our role to make suggestions for law reform in the UK, but the interviews do present a useful picture of some of the controversies in that jurisdiction, at least as they stood in February 2016.

The following suggestions made by UK participants are of interest to the Australian law reform process: (1) suggestions for the conditions under which law reform decisions in this area ought to be made (based on evidence of privacy risks and security benefit, including proper justification for operational cases), subject to transparency issues discussed in 2.6.4 below; (2) ideas for improving oversight and accountability; (3) the importance of a principles-based regime that is less likely to date quickly; and (4) the importance of clarity and comprehensiveness are worth keeping in mind in developing a better legal framework for Australia.

2.5.5 Regulation by design

Only two research participants in operational organisations had a role that enabled them to comment on ‘regulation by design’ within their organisation’s systems. These two participants were asked about the extent to which some of the risks of data analytics could be mitigated through the design of analytical tools as well as the extent to which it was taken into account in their own systems. The two sets of responses are set out in Table 2-13 below.
Table 2-13: Mitigation of issues/risks associated with data analytics/storage systems through design (n=2)

<table>
<thead>
<tr>
<th>Issue</th>
<th>O-T/O (1)</th>
<th>O-T/O (2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and personal information security</td>
<td>Access restrictions and vetting</td>
<td>Access restrictions</td>
</tr>
<tr>
<td>(see Methodology Report 5.2.2, 5.2.5)</td>
<td>External security audit</td>
<td>Only bring in raw information about</td>
</tr>
<tr>
<td></td>
<td>Security monitoring software</td>
<td>targets, through bulk matching</td>
</tr>
<tr>
<td></td>
<td>Security levels analysed as part of design process</td>
<td></td>
</tr>
<tr>
<td>Communications confidentiality (see</td>
<td>Data movements are recorded</td>
<td>Encryption</td>
</tr>
<tr>
<td>Methodology Report 5.2.2)</td>
<td>Not everyone with access rights has the right to move data</td>
<td>Data treated as an asset</td>
</tr>
<tr>
<td>Data integrity (see Methodology Report 5.2.4)</td>
<td>Audit checks for changes</td>
<td>Reliability and accuracy is ‘crucial’</td>
</tr>
<tr>
<td></td>
<td>Actively looking for anomalies / conducting ‘sense checks’</td>
<td>Raw data is never changed</td>
</tr>
<tr>
<td></td>
<td>Close relationship with data providers</td>
<td>No non-trivial data cleaning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incorrect or inconsistent data is flagged</td>
</tr>
<tr>
<td>Regulatory compliance (see Methodology</td>
<td>Meets data security requirements,</td>
<td>‘It is all modelled to replicate all</td>
</tr>
<tr>
<td>Report 5.2.2)</td>
<td><em>Data Protection Act</em> requirements.</td>
<td>information handling and access policies and audit polices*</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing and evaluation (see Methodology</td>
<td>Only on deployment</td>
<td>Yes, technical testing and testing outputs</td>
</tr>
<tr>
<td>Report 5.2.5)</td>
<td></td>
<td>against human produced product.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>‘Officers won’t trust it if it is wrong once’</td>
</tr>
<tr>
<td>Comprehensibility to decision-makers (see</td>
<td>Need to explain to reliability measures such as confidence intervals</td>
<td>Yes, but also need ability to ask complex</td>
</tr>
<tr>
<td>Methodology Report 5.2.6)</td>
<td></td>
<td>questions. Officers need to know enough to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>engender trust.</td>
</tr>
<tr>
<td>Avoiding discrimination (see Methodology</td>
<td>No individual level responses (report on aggregates). But analyse biases</td>
<td>Racial information is captured but no</td>
</tr>
<tr>
<td>Report 5.2.6)</td>
<td>and inequalities as part of role.</td>
<td>bias is applied to it by system.</td>
</tr>
<tr>
<td>Agency inter-operability</td>
<td>Movement towards using data intelligently</td>
<td>Data exportable in a structured format so</td>
</tr>
<tr>
<td></td>
<td></td>
<td>that another agency can use it.</td>
</tr>
<tr>
<td>Re-identification risk (see Methodology</td>
<td>Testing conducted prior to release of aggregate data</td>
<td>It depends</td>
</tr>
<tr>
<td>Report 5.2.5)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost</td>
<td>Yes, when purchase consider value for money and appropriateness of</td>
<td>Need money for technical and human</td>
</tr>
<tr>
<td></td>
<td>package</td>
<td>resources; could do more with more money.</td>
</tr>
</tbody>
</table>

One research participant in the policy group had been involved in a company delivering a new capability to law enforcement agencies. That participant spoke about the analysis, design and consultation conducted to ensure the product met privacy standards:

The company [was] determined to make sure that we would respect and accommodate civil liberties concerns. I went to the most vociferous of Britain’s civil liberties groups ... and I met the director ... and I said ... [we are] setting up a new company that is going to give all these powers to the police. But everything we do is going to respect the ECHR. I understand about necessity, proportionality, and accountability. We’re designing in controls, so that’s in a sense a necessity bid. For somebody to be authorised to start searching ... there has to be an authorisation process that justifies why it’s happening. Clearly, that then needs to take account of proportionality. ... Most importantly, we’ve designed an audit trail so that every action that an analyst takes is recorded and ... cannot be wiped, and can be searched in any follow up inquiry. The response from [organisation] is, why don’t more companies come and do what you’re doing? You’re delivering privacy by design. (P/P A)
Summary and Implications

Only three UK participants commented on regulation by design; they noted features similar to those discussed in the Australian study including access controls and audit checks. The positive reaction by the NGO cited in the last example shows that that particular NGO may have been unaware of the commonness of such measures. Greater publicity of existing measures would have many benefits, including increasing public confidence. There may also be benefits for agencies in sharing ideas for compliance by design with each other. Also of note is the comment by one research participant that ‘[o]fficers won’t trust it if it is wrong once’ and the resulting importance of evaluation prior to deployment.

2.6 Values and Big Data

As in Australia, much of the debate about appropriate legal and regulatory regimes lies in different attitudes and values. Different values and different sources of information can yield divisions between those working in government, particularly in operational roles, and those working on policy in the research/NGO sector. In particular, different people can have different views on the role of consent of data subjects, on the importance of privacy and particularly whether it ought to ‘give way’ to security, and on the need for and importance of transparency in operational contexts. We thus asked research participants with policy roles a series of questions seeking to understand their position in these debates, as well as the sources of their views and understandings, the extent to which they perceived their views as in conflict with others and how they would address any such conflict.

2.6.1 Protections where individual consents to use or sharing of their data (see Methodology Report 5.2.2)

The Policy group were asked specifically for their views on an important policy question, namely ‘what protections, if any, should remain in place in circumstances where an individual consents to the use or sharing of their data?’[P12]. The different categories of responses among the policy group mirrored those in the Australian study. Discussion by operational participants about the role of consent are also included below where relevant.

Consent as crucial. One research participant observed that people ‘shouldn’t be very surprised’ or anxious about the use of data in relation to which consent had been given (P/P). Another research participant (P/P) emphasised the importance of consent in evaluating the appropriateness of collection and use of data. One person in the operational group also mentioned that they work ‘on the basis of informed consent’ (O-T/O). However, another participant in the operational group pointed out that the intelligence community was exempt from the requirement for consent (O-P/O). One participant in the policy group described this exception to the consent requirement as involving ‘societal consent’ due to general agreement that an offender’s data can be used without consent (P/P).

Consent needs to be active, clear and visible, fully informed and unpressured. Four research participants (P/P) emphasised the need for real consent.

Data must be used for a proper purpose. Three research participants (P/P) pointed out that data must be used for a purpose for which consent has been granted. One additional research participant mentioned that data should not be shared between departments without consent of the data subject (P/P).

Some limits. One research participant (P/P) pointed out that there are some things that people cannot reasonably consent to. Another research participant (P/P) observed that the government obligation to protect people’s human rights remains even if consent is given to data collection.

**Data security.** One research participant (P/P) referred to the continuing need to have appropriate protections in place.

**Summary and Implications**

Research participants in the UK (as those in Australia) mentioned issues around the ‘quality’ of consent, continuing limits on its use (including proper purpose) and security requirements. The issue of expiry or revocation was not raised in the UK study. One interesting issue explored by some research participants is how consent requirements fit with national security and law enforcement exceptions. The idea of ‘societal consent’ could be a useful concept here.

2.6.2 Attitudes to privacy (see Methodology Report 5.2.2)

Participants were asked to comment on the balance between privacy and threats such as child kidnapping, child sexual abuse or terrorism [O21, P14]. Table 2-14 summarises their responses.

**Table 2-14: Policy participants’ attitudes to privacy by organisation sector (n=8)**

<table>
<thead>
<tr>
<th></th>
<th>Research/NGO/ Private</th>
<th>Independent</th>
<th>Government</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need to follow rules (including oversight, necessity and proportionality requirements)</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Privacy not important where inferences based on aggregates</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Privacy should give way in the face of such threats (if justified)</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Need to find balance in circumstances</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Even in extreme circumstances, invasions of privacy should be targeted</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

* Multiple responses can be coded for each research participant.

One research participant explained the balance between security and privacy as follows:

> The graph I always draw ... it’s a very simple graph, you have two axes, one of which is security, ... one of which is privacy and there’s a limiting curve, which is the most of one you could have at any given value of the other. That for a certain value of security, you simply cannot allow more privacy than a certain amount and the other way around. The debate is often phrased around there that we are on that edge. We’re actually almost certainly somewhere comfortably inside. So we could actually improve both the security benefits and reduce the privacy costs simultaneously. (P/P A)

The idea that both security and privacy are important and necessary for each other is captured in RUSI 2.3: ‘There is no privacy without respect for security; there is no liberty without respect for privacy; security requires both certain liberties and privacy. It is therefore unfruitful (indeed misleading) to cast debates about privacy, liberty and security as a matter of choice or ‘balancing’ between these rights, still less to think of trade-offs between these rights.’
Summary and Implications

Research participants in both the UK and Australia had varied views on the importance of privacy, particularly in the context of serious, imminent threats. Similarly, no-one in the UK sample expressed the view that privacy should always be prioritised, although the view was expressed that security threats never justified untargeted intrusions on privacy. While the UK study revealed differences in the relative importance of privacy between different sectors (research/NGO compared to government/independent, the latter being more likely to say privacy should give way), research participants from both ‘sides’ emphasised the importance of following rules relating to oversight, necessity and proportionality. See also 1.1.

The observation set out in the extended quote is also noteworthy – there are ways of improving both privacy and security in which neither is sacrificed.

2.6.3 Privacy versus Security: A scenario (see Methodology Report 5.2.2)

In order to gain greater insight into the ways in which research participants with policy or joint operational/policy roles believed that concerns around privacy (including surveillance) do or ought to interact with concerns around security, we presented research participants in that group with a scenario:

Lucy is an 8 year old girl who has been kidnapped from her home in London. All avenues of traditional physical surveillance and canvassing of the area so far haven’t produced any leads. How do you feel about the immediate and expeditious use of Big Data tools in these circumstances? [P13]

This was essentially what this question set out to test. After an initial response to this scenario or where the research participant asked for examples, and in order to further test where research participants would draw lines, research participants were asked a series of more specific questions, in particular their response to:

a) A metadata (secondary data) search of all known kidnappers with previous arrests in the area matched against CCTV footage from public and private sources in London on the day of the kidnapping

b) Collection of data and monitoring of all known kidnappers including known addresses, registered telephonic devices, social media accounts and email accounts

c) Facial recognition deployed on CCTV footage across all Sydney and surrounding areas, and multiple social media networks, in an attempt to identify Lucy

d) Metadata from all devices of all family members of Lucy, her neighbours, and people seen visiting the house that day (including a postal worker, package delivery service, water meter inspector).

Table 2-15: Responses to general kidnapping scenario and specific prompts (n=7)

<table>
<thead>
<tr>
<th></th>
<th>Agree to use tool/s</th>
<th>Agree to use tool/s with caveats</th>
<th>Reluctant to use tool/s</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial response</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Prompt (a)</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Prompt (b)</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Prompt (c)</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Prompt (d)</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

* One research participant in the policy group was not asked this question due to time constraints.

** Some respondents mentioned general caveats in giving a positive response initially. Where these were repeated in relation to specific prompts (including by reference), the research participant was placed in the ‘agree to use tool with caveats’ column. However, where the research participant did not mention the earlier general caveat but gave an unconditional positive response to the prompt, they were put into the ‘agree to use tool’ column.
Three research participants had difficulty answering the question in the form in which it was phrased. One (P/P) answered it in the position of a judge asked to consider whether a warrant authorising that should be upheld. Two (both P/P), in a joint interview, changed the context to national security rather than law enforcement (so ‘Jack is a 15 year old guy who has taken off for Syria’) due to that being the context in which they operate. Because of the change in format, none are included in the table. However, we included the first participant in our qualitative analysis below, given the shift was merely as to context (thus n=8 for the qualitative analysis). The joint response is analysed separately given it represented a complete change to the scenario.

**Initial responses (prior to prompts)** Research participants gave a variety of suggestions for investigators, including:

- Start by investigating her family (2 P/P) or others living in the house (O-T/O).
- Could use location data on Lucy’s phone (P/P) as well as internet and communications with Lucy (O-P/O).
- Investigate phone records to and from the house and use Automatic Licence Plate Recognition near the property (O-T/O).
- Look at which mobile phones were active in the area where the kidnapping took place (O-P/O).
- Investigate whether it was a drug deal / debt situation (O-T/O).

Research participants also suggested several general caveats (not otherwise mentioned in the scenario) that should apply, including:

- It had to be a limited amount of data (P/P).
- There had to be some connection between the individuals on whom data was collected and the crime (P/P).
- The investigation should be done in stages, ‘you don’t have to start with extreme measures’, so one could begin with questioning suspects, then go to surveillance, before intercepting communications (‘really the most extreme of invasions of privacy’) (P/P). This resonated with another research participant’s response that Big Data, particularly where it necessitates bulk collection of everyone’s data in advance, should not be the first answer to the scenario (P/P).
- Necessity, proportionality and accountability remain important (P/P).

There were also specific caveats suggested for different prompts, these are set out below:

**Prompt (a)**

- There would need to be some reason linking the person with the crime beyond a previous conviction, for example it could be a similar modus operandi (P/P).
- There would need to be evidence as to reoffending rates in order to raise reasonable level of suspicion (P/P).
- It would depend on how many ‘known kidnappers’ there were due to the proportionality requirement (P/P, who also questioned whether there was power to keep a database on arrests as opposed to convictions).
- It would depend on any regulatory requirements for access to private CCTV cameras (P/P).

One research participant (P/P) pointed out that a more targeted surveillance system would put under surveillance people who were considered a threat (e.g. kidnappers at risk of re-offending).

**Prompt (b)**

- It would need to be proportionate, so could not be done randomly but on a judgment as to which particular people were under suspicion (O-P/O).
- Only for ‘high risk’ offenders. (P/P)
- Not proportionate unless ‘known kidnapper’ operated similarly to a sex offender list (P/P).
• There would need to be evidence as to reoffending rates in order to raise reasonable level of suspicion (P/P)

**Prompt (c)**

• Consent from Lucy’s family (P/P)
• Photos deleted at conclusion of investigation (P/P)
• Only if it was feasible and sufficiently high quality, which is doubtful (O-P/O, P/P)

**Prompt (d)**

• Only those who had acted in a way to put themselves under suspicion in that particular investigation (3 P/P).
• Only if you can prove a link to the people whose metadata is used (such as contact with Lucy) (P/P) or a basis for reasonable suspicion (P/P).
• Only if there was a ‘bloody good case’ that made it proportionate (P/P)

Research participants were then asked whether two changes would alter their response. In particular, they were asked whether it would make a difference if there was a suspicion of paedophilia and whether it would make a difference if there was a suspicion that the kidnapping was linked to terrorist activity (for example, an intent to blow Lucy up in a public place).

Most (6/8) research participants did not believe it would make any difference to their responses if there was a suspicion of paedophilia (other than changing the pool of suspects). One research participant (P/P) pointed out that more powers would be authorised for a more serious offence due to the proportionality principle. Other research participants pointed out that paedophiles are more likely to be under ongoing surveillance (P/P) and that it may affect the reoffending profiles and thus the justification for surveillance/interception (P/P).

Most (7/8) research participants said that changing the context to terrorism would not make a difference to their answers. One research participant (P/P) again noted that more powers would be authorised for a more serious offence due to the proportionality principle. Two participants (both P/P) made the point that terrorists are more likely to be under ongoing surveillance.

In the ‘Jack’ scenario, it was suggested (P/P) that the appropriate course would be to use powers other than access to Bulk Personal Datasets initially. Bulk Personal Datasets could then be used if, for example, those inquiries lead to a phone number that needed to be linked to a name or address. If it were necessary to do so, CCTV cameras could also be set up at a house at which Jack was believed to reside, but only if this were proportionate bearing in mind the other people whose movements would be captured. This may require the cameras to be switched on and off depending on who was present. Generally speaking, the least intrusive techniques should be used before more intrusive techniques.

**Summary and Implications**

As in Australia, most research participants gave the same answers to the scenario whether the context was kidnapping, child sexual assault or terrorism. There were some important differences in the UK responses, including the emphasis on proportionality, the suggestion that data be deleted when it was no longer needed, the suggested need for evidence of reoffending to draw a link with ‘known kidnappers’, and the fact that many potential suspects would already be under surveillance. Also, there was some scepticism about the effectiveness of the hypothesised CCTV face recognition matching tool (in particular by one participant who has developed video analytic tools and one in an operational role).

2.6.4 What transparency is required (see Methodology Report 5.2.8; 3.8)

We asked research participants with policy roles and joint operational/policy roles to comment on the extent to which there should be transparency about the nature of data collected or the
algorithms employed in analysis, both within an agency and more broadly [P15]. The results are shown in Table 2-16.

Table 2-16: Views of research participants with policy roles on transparency of data and algorithms (n=11)

<table>
<thead>
<tr>
<th>Types of data collected should be transparent</th>
<th>Data envelope / some information about data should be transparent</th>
<th>Data should not necessarily be transparent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithms should be transparent</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Algorithm envelope / some information about algorithms should be transparent</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Algorithms should not be transparent</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

As in Australia, the importance of not compromising operational effectiveness or the risk of criminals gaming the system was mentioned by most (7/11) research participants. Anderson (10.4, 10.5) noted traditional intelligence agency aversion to public transparency, even where that position was contrary to the agency’s own interests, but this is now softening. RUSI also noted the cultural change in this respect over time (at 2.49). One research participant was sceptical due to the lack of demonstrated harm caused by greater transparency today (due in part to Snowden) than historically (P/P).

In relation to data, some research participants discussed the possibility of post-surveillance notification, where data subjects would be told that they were under investigation after the operation had concluded. Two research participants (both P/P) were in favour of this, one on condition that it does not interfere with a current investigation. The contrary position was put by another research participant (P/P). See also section 3.8.1.

One research participant (P/P government) felt that, while algorithms could not be made transparent without facilitating gaming, *the fact that machine learning is used* to help tackle a particular type of crime ought to be disclosed (P/P). Another felt that, while algorithms should generally be kept confidential, some information may need to be disclosed in court in some circumstances (O-P/O). Also in relation to algorithms, one research participant (P/P NGO) suggested a combination of transparency (e.g. processes through which algorithms and queries are generated) and safeguards (e.g. to prevent algorithms being used in a discriminatory way).

Most (8/11) research participants believed that there needed to be transparency within government, at least for the analysts using them and the agencies overseeing them, including those who would have full transparency in any event (P/P):

> [W]e need to think about algorithmic accountability and what happens there particularly in places where you can’t be [transparent] about algorithms. (P/P A).

> The oversight agencies ... can’t really offer proper oversight unless they know. One of the things that we’ve been campaigning for is for the new oversight body to have access to technical systems and also to specifically oversee the way in which big data is being used. (P/P B)

> Yeah, the people who are tasked with overseeing will again have signed the [Official Secrets Act], they will understand that they will need to keep that secret, and in order for them to do their jobs properly they will need to understand exactly how it all works. (P/P C)

One research participants expressed some qualifications about even intra-government transparency:
It should certainly be understood by the people directly involved with it ... monitors or reviewers should certainly be able to crawl all over it to understand exactly what’s being done. I’m not sure it should be necessarily accessible to everybody in government. I think one should assume that anything that is accessible to everybody in government is accessible for everyone. (P/P D)

Additionally, two research participants (in the same organisation and interview) emphasised the importance of trust. They were discussing the possibility that an independent oversight agency have direct access to computers at the operational agency:

... the only people with the skills to use certain systems work within the intelligence services, so what we do is to make sure that they are checking the systems themselves, the people with the skills. Then we come one step back from that and making sure that their checks are adequate. (P/P E)

At the end of the day there’s got to be trust somewhere. My anxiety about those people who want to put into the oversight body the skills of exploring all the computers is that once you actually start if you’re not careful you start a battle. (P/P F)

Summary and Implications

In both Australia and the UK, transparency raises questions about competing priorities – operational effectiveness, trade secrets and democratic accountability. Although in the UK some research participants did not believe in transparency about the types of data collected, there was still more concern about disclosure of algorithms than disclosure of data types.

Noteworthy points arising from the UK study include the discussion about oversight and trust and the inevitable reliance on co-operation between oversight and operational agencies. Fuller transparency (for example, direct access to computers) risks undermining that trust and the joint construction of oversight systems. The possibility of post-surveillance disclosure was also a new finding in the UK study.

2.6.5 How views align with others

Research participants with policy and joint operational/policy roles were asked to comment on how their views about the design and regulation of Big Data aligned with the views of other stakeholders [P16].

Some of the research participants referred to co-operation among a coalition of rights-based NGOs that share similar positions. As in Australia, there often were differences between this community and the government (including the Home Office and the agencies), a split that was also noted in Anderson 1.7 and RUSI 5.2. However, one research participant felt aligned both to NGOs and to some thoughtful members of GCHQ, but not the Home Office (P/P). And another research participant noted that ‘... we are in a relatively good position here in this country. I think there’s a fair degree of balance. There’s a fair degree of understanding of the other side.’ (P/P A).

Some participants (across sectors – government, independent, NGO) commented on the fact that the process going towards the Investigatory Powers Bill had been helpful:

I think there’s been a realisation that the two sides aren’t as far apart as they first thought, but I think there’s still a way to go, because for example, we get certain moves from the government who, when they draft legislation they’ll move a certain way, but they won’t move further past that point. So they’ll move a certain point to give the appearance of listening, but they won’t move any further, which is frustrating, but I think there has been a slight moving together. (P/P B)

I’ve spoken to a number of the NGOs and when we sit down together we actually are trying to do the same thing. We are trying to protect privacy and so we do have an awful lot in
common when we sit down. ... It hopefully provides them with reassurance. It provides me with reassurance that they’re not just trying to create anarchy. (P/P C)

We attend conferences together and they express their views. You don’t find much difference in view. ... I think one of the definite differences, they don’t trust that the agencies are not misusing the information that they hold. They take a lot of convincing that they actually do want to obey the rules and they don’t want to invade privacy more than is actually necessary. (P/P D)

The main stakeholders who remain kind of slightly outlying are clearly those with big interest in civil liberties where they’re not entirely convinced, although they have moved quite a long way since the early days of the Snowden revelations. ... They’ve accepted that where it can be shown that it’s targeted and proportional then you need to do this kind of stuff. They are still not convinced that the net isn’t being cast too widely in some of these operations. ... [The UK reports and debate] hasn’t necessarily narrowed the gap in terms of Big Data and bulk data analysis but it has certainly narrowed the gap in terms of ‘well if you must do this we want to see some very firm oversight and authorisation getting the judges to sign the warrants and all the rest of it.” [Q: It’s focused it?] Yes. (O-P/O E)

But barriers and disappointments remain:

I think we’ve been trying to sit down at a table with these people and some of my colleagues in the NGO space have achieved relationships with people. But less so in the intelligence services than in law enforcement. ... I just don’t think that they [intelligence agencies] think we have any legitimacy. At the moment, I remain of the conclusion that there’s no compromise to be reached with intelligence services in terms of trying to come to a common understanding about how best to achieve these things. (P/P F)

The only way to reassure the NGOs would be to get them vetted, to bring them into the agencies, to put them in a trusted position. But then they wouldn’t be able to do their job because they’d be part of the system. ... I think as a country we need people coming up with an opposing view. (P/P G)

... there is no doubt that there is a great deal of mistrust by virtue of the fact that the policy is neither confirmed or denied. (P/P H)

There is certainly a terrible lack of technical expertise or interest in parliament and the government. So really, parliamentarians are at the mercy of the agencies and there’s very little scope for critical input and an unwillingness to critically engage and therefore to set out where maybe there should be limits. ... [H]opefully, some of these matters will be settled in the courts. (P/P I)

Summary and Implications

Although the same differences in opinions existed in the UK as in Australia, the public process through which the law has been changed (including the three reports leading up to the Investigatory Powers Bill) seemed to have narrowed the gap to some extent, or at least clarified the areas of disagreement. However, there remained some distrust between parts of the government and agencies, and the NGO community.

2.6.6 Resolving conflicts in values

Research participants were asked how conflicts in values might be resolved. A number of suggestions were offered.

Structured conversations. Some research participants described past processes or made suggestions for more structured conversations between government and stakeholders about government’s use of data and analytics.
One research participant (working for government in a policy role) described **public workshops concerning the government’s use of data science**. In these workshops, the government’s data ethics framework was tested and participants could respond to different scenarios. These workshops included an educational element, but also revealed (to that research participant) some insights into the public’s views. For example:

They’re kind of like fine if companies do that because ... we’ve kind of signed that away, we’re clear what we’re getting from them. Whereas they don’t think that governments should be doing it ... So it’s linked to people’s views about what people are going to use it for and what the intervention is going to be. ... [Y]ou can’t talk about Data Science unless you talk about, well, is someone going to get arrested at the end of the decision. ... [L]ots of people just don’t believe you can make these correlations that you can infer things from Big Data. Lots of people question ‘why can’t you use traditional investigative methods’. ... People are very worried about false positives. ... [P]eople ... were happy for decisions to be automated around ... fishing licence grants or whatever it is because it was kind of benign. They were quite happy for people to use more intrusive data for these sorts of things but then there has to be checks and what happens afterwards. (P/P A)

That research participant also suggested establishing an ethical council to develop policy principles around data, algorithmic accountability, and technical standards (P/P).

A second participant (P/P) described the benefits of different stakeholders coming together to solve data-related problems in appropriate ways:

When I [understood] what the IP address matching this was, I was like yes, absolutely, there is a problem here, we need to find a way of tackling it, here’s a few ways we can tackle it.

What would be much better actually if one could have a proper conversation which essentially said here are the things we’re trying to do. This is why we need to be able to do them, can we have an open conversation about how we can go about doing them. ... How do we actually try to get both security and privacy? (P/P B, giving the example of identity assurance without identity cards.)

A third participant also raised the importance of a ‘safe space where the two sides can get to understand each other’s views’. (P/P C)

**Empirical testing.** One research participant suggested independent reviews into the efficacy of mass surveillance methods (P/P), which can work where the disagreement is based on empirically provable facts, for example as to effectiveness. However, challenges remain where examples of effectiveness cannot be published due to the need to maintain operational secrecy.107

**Summary and Implications**

As in Australia, differences in values are ultimately settled through democratic elections (Australia report 2.6.6). However, in the UK there were constructive suggestions around further conversations and dialogue, including public workshops, an ethical council or collective problem solving. In some circumstances it may be possible to conduct empirical testing as to matters of fact on which there is disagreement (such as the effectiveness of particular techniques) to the extent this can be done without compromising operational secrecy.

---

2.6.7 Source of views

Table 2-17: Sources of views of Policy group by organisation sector

<table>
<thead>
<tr>
<th>Source of views</th>
<th>Private/ Research/ NGO</th>
<th>Independent</th>
<th>Government</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional/personal experience, knowledge</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Evidence / Academic papers / Reports</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Media/blogs</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Broad consultation</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Contact with experts</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Whistle-blowers</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

* Multiple responses can be coded for each research participant.

As in Australia, research participants relied on personal and professional experience as well as a range of external sources. Due to the publication of a series of reports in the UK leading up to and following the introduction of the Investigatory Powers Bill, these and related academic discussion was important for some participants. Experts and whistle-blowers were also mentioned.

Summary and Implications

Research participants in the UK formed their views based on similar sources to Australian participants. The recent reports leading up to and following release of the Investigatory Powers Bill were also important in the UK.
3. BIG DATA, LAW ENFORCEMENT AND NATIONAL SECURITY: 
THE LEGAL ENVIRONMENT IN THE UNITED KINGDOM

This chapter discusses features of the UK legal framework relevant to Big Data, law enforcement and national security.

The chapter is divided into eight sections that reflect the lines of inquiry introduced in Chapter 5 of the Methodology Report, generally referred to as the ‘lens’ in this discussion. The sections therefore address aspects of the regulatory framework on the following topics:

1. Is access for data mining enabled?
2. Are legal controls comprehensive and proportional?
3. Are legal rules clear, principle-based, consistent and instructive?
4. Is integrity of data and analysis supported?
5. Are data and systems protected?
6. Is accountability maintained?
7. Are principles and rules regularly reviewed?
8. Is there a sufficient measure of transparency?

While the ‘lens’ is used to structure this discussion, it is important to emphasise that it is only used to inform the lines of inquiry, and not as a tool to assess the current framework. It is used to focus the inquiry on key elements which, if collectively present, would be indicative of a framework that:

- supports the effective use of advanced analytics and large data sets for law enforcement and national security purposes,
- while respecting the rights and interests of all stakeholders (including data subjects and the broader community and economy);
- reflects proportionality and evidence-based justification and decision-taking; and
- ensures comprehensive identification and management of risk and opportunities.

The indicators are not presented as a comprehensive or final list. They provide structure to the analysis but are not meant to restrict the broader enquiry or the ongoing debate about an appropriate framework.

The UK’s legal environment regarding data is highly complex and detailed. The objective of this chapter is not to capture the detail or to comprehensively map access rules and exchange mechanisms but rather to trace the broader features and contours of the framework that are of particular relevance to this study.

The study focuses on publicly available data and especially on the three reports relating to surveillance and access to telecommunications data outlined in Chapter 1 and the Investigatory Powers Bill 2016. The legal position is reflected as at 26 May 2016 and references to the Investigatory Powers Bill are to the version of the Bill introduced in the House of Commons.

3.1 Is access for data mining enabled?

The first line of enquiry addresses access to data, subject to the governance and control mechanisms set out in 3.2–3.8 below, for purposes of analysis using Big Data techniques. It considers whether the framework enables access, subject to those mechanisms, to:

1. relevant datasets held by government agencies (domestically and internationally),
2. ‘open source’ data,
3. relevant privately-held data, and
4. datasets held by foreign agencies.

in a manner that allows data mining.

This section considers the parameters for this type of access, while the discussion in 3.2, addressing controls that are imposed on access, use and other dealings with data, considers features of the
legal nature of some of the controls, and the degree to which these require the question of proportionality to be taken fully into account.

This discussion now focuses briefly on access to each of the four types of data noted above.

3.1.1 Access to government-held data

‘Government-held data’ refers to information stored by all levels of government.

UK intelligence and law enforcement agencies enjoy extensive access to a wide range of government-held data. The Police National Computer (PNC) provides an example of the extent of the data systems.

The PNC is a computer system for police forces in the United Kingdom, owned by the Association of Chief Police Officers (ACPO) and managed and controlled by the Home Office.\textsuperscript{108} Police forces and other law enforcement agencies, approved organisations and government departments, such as intelligence agencies and the Home Office, can access the system for specific purposes.\textsuperscript{109}

The PNC, which was established in 1974 to store details of stolen vehicles, has evolved and grown over time. In recent years, the range of facilities, level of detail and potential value of information stored on the PNC has grown considerably. The system can link into a number of separate databases and can access a range of records such as:

- personal descriptions (not given by PNC bureau)
- bail conditions (not given by PNC bureau)
- convictions
- custodial history
- wanted or missing reports
- warning markers
- pending prosecutions
- disqualified driver records
- cautions
- drink drive related offences
- reprimands
- formal warnings
- vehicle details
  - registration number
  - make
  - colour, and
  - modifications of vehicles as well as details of cherished transfers of registration plates
- registered keeper of vehicle details:
  - name
  - address
  - date since acquired
- Driver and Vehicle Licensing Agency markers
- Police reports, and
- Vehicle insurance details\textsuperscript{110}

The PNC also holds details of people on the National Firearms Certificate Holders register.\textsuperscript{111}


The PNC supports a number of applications, such as:

- **QUEST** (Querying Using Enhanced or Extended Search Techniques), which enables users to search the names database and to identify suspects on the basis of partial physical descriptions and personal features.
- **VODS** (Vehicle Online Descriptive Search), which enables users to search for specific vehicles using criteria as registration, colour and postcode.
- **ANPR** (Automatic Number Plate Recognition), which is linked to an extensive CCTV camera network and enables identification of vehicles of interest based on visual images of a number plate, combined with other PNC data; and
- **CRIMELINK**, which enables crime and intelligence analysts to identify patterns and links in crimes across the UK.\(^{112}\)

In addition to the PNC, the UK also maintains the Police National Database (**PND**). The PND was rolled out as a result of the recommendations of the Bichard inquiry into child protection procedures in the Humberside Police and Cambridgeshire Constabulary.\(^{113}\) This database holds more background information relevant to crimes, rather than hard criminal justice data.\(^{114}\) It holds, for example, police intelligence such as details of criminal investigations that did not lead to a conviction.\(^{115}\)

Access to data includes access to non-clinical patient data on the NHS to assist with the tracing of individuals for the purposes of law enforcement.\(^{116}\) Strict criteria must be met where a request for such access is made by the Police, the National Crime Agency and the Home Office. Courts may also order such access. Generally the information will only be released where the alleged crime is serious or involves the abuse of the NHS. However, where the request is lodged by the NCA ‘the criteria for it to be a ‘serious crime’ is not applied as the purpose of the agency is to investigate serious and organised crime.’\(^{117}\)

While the PNC and PND provide central access to key crime and justice-related data, research participants indicated that a number of relevant databases are still held separately and needed to be accessed and interrogated individually. Other categories of government-held crime data accessed within operational organisations were described in interviews (2.1.2).

### 3.1.2 Access to ‘open source’ or publicly accessible data

The use of social media data for law enforcement purposes is regulated under the *Data Protection Act 1998*. Other laws such as the *Human Rights Act 1998* and the *Regulation of Investigatory Powers Act 2000* may also apply.\(^{118}\) The *Data Protection Act 1998* introduces important safeguards to ensure

---


\(^{116}\) Health and Social Care Information Centre (UK), *Registers of approved data releases: Guide to tabs, column descriptions, key terms and abbreviations* (2015) 10: ‘The NBO’s (National Back Office’s) primary task is to ensure that demographic information on the Personal Demographics Service is accurate so that the NHS can use it for providing care.

The NBO also provides strictly circumscribed non-clinical information to assist with the tracing of individuals for the purposes of law enforcement where certain criteria are met, including where the exemption under section 29(3) of the Data Protection Act applies or where it is compelled to do so by a court order.’


\(^{118}\) Parliamentary Office of Science and Technology (UK), ‘Social Media and Big Data’ (POSTNOTE, Number 460, March 2014) 3.
data is appropriately handled by organisations. As noted in Chapter 1, the Act however provides an exemption from relevant provisions when national security interests are engaged.\textsuperscript{119}

The UK maintains various capabilities to access and mine social media. For the Metropolitan Police, for example, these include the All Source Hub (ASH), the Communications Exploitation Group (CEG), and Counter Terrorism Internal Referral Unit (CTIRU).\textsuperscript{120}

- **ASH** provides a platform enabling the analysis of both open-source and police databases. It is primarily focused on threats of disorder and domestic extremism. Ahead of the 2012 London Olympics, for example, it enabled the preparation of intelligence reports based on the analysis of ‘31 million items across 56,000 social media platforms.’ It also enables the use of photographs and geotags posted by foreign fighters in Syria to identify their likely locations and to build material and evidence for investigations.\textsuperscript{121}

- **CEG** focuses on lawful intercepts, cyber-operations, and the attribution of communications data. It is particularly focused on detecting hacking, for example hacking attacks on the City of London or by extremists.\textsuperscript{122}

- **CTIRU** seeks out online terrorist material and also receive referrals from the public, partner agencies and officials. They remove more than 1,000 items per week from websites, for example terrorist propaganda and instruction material on how to build bombs.\textsuperscript{123}

### 3.1.3 Access to privately-held data

A significant source of data for government agencies is data held by private corporations. The *Intelligence Services Act 1994* and the *Security Service Act 1989* provide the legal basis for the acquisition of such data. It may be acquired covertly and overtly and may even be purchased from companies and vendors and obtained from foreign counterparts.\textsuperscript{124} Specific provisions apply in relation to telecommunications information.

*Telecommunications information*

RIPA, likely to be amended by the *Investigatory Powers Bill* discussed in 3.1.5, currently provides the legal basis for the lawful interception of communications, access to communications data, surveillance, the use of undercover agents and informers, and access to protected data. This Act responds to the privacy protection under the *Human Rights Act 1998* by setting out the grounds for justification for such intercepts. These grounds include national security interests, including safeguarding the economic well-being of the UK in circumstances relating to national security, and the prevention and/or detection of serious crime.\textsuperscript{125}

RIPA distinguishes between communications data (metadata) and content. Officials within the organisation seeking access to communications data may authorise such access. As RUSI noted:

> Part I, Chapter II of RIPA 2000 covers the acquisition and disclosure of communications data. Only certain organisations are able to request communications data from CSPs. They include police forces, the NCA, HMRC and the SIAs, as well as local authorities. Only persons designated under the Act may authorise access to communications data, and only for certain purposes (the persons and purposes vary according to the organisation in question).\textsuperscript{126}

---

\textsuperscript{119} Data Protection Act 1998 s 28. See also RUSI Report 76 [4.15].


A warrant issued by a Secretary of State is generally required to access content. RUSI summarised how this works in practice:

In practice, the Foreign Secretary, the Home Secretary, the Secretary of State for Northern Ireland, the Defence Secretary and the Cabinet Secretary for Justice for Scotland authorise interception warrants. The secretary of state must make a judgement whether or not the interception is both necessary and proportionate. The Home Office Code of Practice notes that ‘Interception of communications will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other means’. RIPA also distinguishes between ‘internal communications’ (that are both sent and received in the UK) and ‘external communications’ (in which either the sender and/or recipient are outside the UK). Communications that are internal may only be intercepted under a warrant issued in terms of s 8(1) of RIPA. The warrants must name or describe the subject of the interception, as well as identifying factors that will be used to identify the communications to be intercepted. External communications can be accessed by a warrant granted under s 8(4) of RIPA. Such a warrant does not need to name the subject of interception and does not need to impose a limit on the number of external communications which may be intercepted. While s 8(1) warrants are primarily investigative tools, s 8(4) warrants are used for intelligence purposes to collect bulk data. Section 8(1) has, however, also been interpreted in a manner that lends it to broader application. It has been used to issue thematic warrants covering a group or network of persons. This is possible as RIPA defines a person as ‘any organisation or any association or combination of persons’. The ISC expressed concern as to the extent that thematic warrants are used and around associated safeguards. It advised that it should be used sparingly and should be authorised for shorter periods than standard 8(1) warrants. The Anderson review, on the other hand, encouraged the use of thematic warrants but within strict limits, especially regarding the power to modify the warrant. It advised that the power to make major modifications such as adding a person or premises should be for a Judicial Commissioner.

The application of section 94 of the Telecommunications Act (directions in the interests of national security) to access bulk communications data has also been controversial. This section stipulates:

1. The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom.

2. The Secretary of State shall lay before each House of Parliament a copy of every direction given under this section unless he is of opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person.

---

This section applies to OFCOM and to providers of public electronic communications networks.

Directions were apparently issued that enabled agencies to access bulk data. Possibly due to their sensitivity in terms of section 94(4), these are not publicly available.

In its 2014 report, the Interception of Communications Commissioner disclosed that he accepted a request from the prime minister to oversee section 94 directions. In the wake of litigation brought by Privacy International regarding the use of section 94 powers, it has gained access to redacted versions of formerly classified documents. These were released in early 2016 for purposes of the litigation and were published by Privacy International.

3.1.4 Access to information by, and from, foreign governments and entities

The UK agencies share intelligence with its Five Eyes and other international counterparts. As the Anderson report noted:

The obtaining and disclosure of information by the security and intelligence agencies is governed by:

(a) SSA 1989 and ISA 1994, which require the agencies to ensure that information is obtained and shared only in pursuit of their functions; and
(b) HRA 1998, which requires them to operate in conformity with ECHR rights including in particular Article 8.

While acknowledging that there are very good reasons why the UK’s intelligence agencies share information with partner agencies in other countries, the RUSI report stated that currently ‘there is insufficient clarity over the powers and safeguards governing the exchange of data and intelligence between international partners.’ The report also noted that, as far as cross-border law enforcement is concerned, ‘current legal-assistance processes are burdensome and, crucially, slow in comparison to the pace at which online threats can develop.’ The report therefore recommended urgent improvements ‘to expedite the mutual legal assistance treaty (MLAT) process and, in particular, to the UK–US process in managing data requests.’

The ISC report also expressed concerns regarding the lack of statutory underpinning for these exchanges with foreign agencies:

As set out previously, under the Intelligence Services Act 1994 and the Security Service Act 1989 the Agencies are authorised to obtain and disclose information in support of their functions. One of the ways in which they use this power is to exchange information with other intelligence agencies. However, the legislation does not contain any detail as to how that exchange should take place or how it should be authorised.

Those we have taken evidence from throughout this Inquiry have accepted that, due to the international nature of the threats facing the UK, sharing intelligence with our allies is a fundamental part of the Agencies’ work. However, most of our witnesses felt that current intelligence-sharing arrangements are insufficiently regulated, and some suggested that this

---

136 Anthony May in Interception of Communications Commissioner’s Office, Report of the Interception of Communications Commissioner House of Commons Paper 1113, Session 2014-15 (March 2015) [10.2]: ‘My oversight of section 94 will be on a non-statutory basis in the short term, but I hope that this can be addressed in the next Parliament.’ (‘Report of the IOCCO’)

137 The matter is before the Investigatory Powers Tribunal and focuses on the use by MI5, MI6 and GCHQ of section 94 powers. See <https://www.privacyinternational.org/node/854>.


might provide a mechanism by which the Agencies could circumvent UK legal constraints and human rights protections. Privacy International, for example, argued that ‘UK law places no meaningful restrictions on the information that the intelligence and security services can share with and obtain from this [Five-Eyes] network’. Concerns over intelligence-sharing arrangements have increased since revelations regarding the US-run PRISM programme. At the time, the Guardian alleged that access to the PRISM programme ‘would appear to allow GCHQ to circumvent the formal legal process required to seek personal material such as emails, photos and videos from an internet company based outside the UK’.  

RUSI also noted Sir Nigel Sheinwald’s appointment in September 2014 as the prime minister’s special envoy on intelligence and law enforcement data sharing:

His role was to ‘work with foreign governments and US CSPs to improve access to data across different jurisdictions for intelligence and law enforcement purposes’. This work has concentrated on building new strategic relations with the companies, working with the US government and others to develop new solutions to current legal and jurisdictional problems. Co-operation is certainly present, says Sheinwald, but remains ‘incomplete’. There is scope to streamline the process by which the SIAs in the UK seek communications data direct from US CSPs, and many companies are examining their own technical solutions to speed up the processing of such requests.  

RUSI supported the practical reforms suggested by Sir Nigel Sheinwald to the existing mutual legal assistance treaty between the UK and the US, to include the greater standardisation of processes, training and improved guidance. It also expressed support for the investigation of a new and wider international framework between like-minded democratic countries with the aim of allowing law enforcement and intelligence agencies more rapid access, under agreed restrictions, to relevant data in cases of serious crime and for urgent counter-terrorism purposes.

3.1.5 Investigatory Powers Bill and access to data

The Investigatory Powers Bill (IPB) does not dramatically increase access to data compared to current powers and practices. It modernises definitions (see Chapter 1), clarifies the range of available powers and subjects their exercise to a range of control measures, including a double-lock system of official approval and judicial review based on tests of necessity and proportionality, discussed in 3.2. The following Table 3-1 provides a brief summary of aspects of control measures linked to key access powers:

---

### Table 3-1: Control methods for types of data

<table>
<thead>
<tr>
<th>Communications-related data</th>
<th>General controls</th>
</tr>
</thead>
</table>
| **Communications data**
• Described as the ‘who’, ‘when’, ‘where’ of a communication and not its actual content
• IPB modernises definitions and adds ‘Internet Connection Records’ (new record-keeping obligation) | • Secretary of State may by notice require a telecommunications operator to *retain* relevant communications data if the Secretary considers that the requirement is necessary and proportionate for one or more stated purposes
• Before giving notice the Secretary must consider a range of practical matters including the impact on the provider and must take reasonable steps to consult the operator
• Retention period limited to 12 months
• Operator may request the Secretary to review the decision or aspect of it and the Secretary must consult the Technical Advisory Board and the Investigatory Powers Commissioner before determining the matter
• Designated senior officer of a relevant public authority may issue a targeted authorisation empowering officers of authority to access communication data if it is considered necessary and proportionate
• Such access may be subject to a request filter |

<table>
<thead>
<tr>
<th>Encrypted data</th>
</tr>
</thead>
</table>
• Existing powers to require decryption under RIPA | • Secretary may issue a technical capability notice to an operator requiring among others, the removal by that operator of electronic protection applied by it or on behalf of it to any communications or data
• Before exercising the power the Secretary must consult with the affected persons and the Technical Advisory Board |

---

148 *IPB* cl 54 defines ‘internet connection record’ as communications data which (a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and (b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person). The new obligation has been criticised as potentially highly intrusive, costly and doomed to be unsuccessful, especially given that users may use a range of tools (Virtual Private Networks, The Onion Router etc) to evade logging meaningful records. See Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill Report*, House of Lords Paper 93, House of Commons Paper 651, Session 2015-16 (2016) [89]-[156].  
149 *IPB* cl 78.
150 *IPB* cl 79.
151 *IPB* cl 78(3).
152 *IPB* cl 80: The Board must consider the technical requirements and the financial consequences, for the operator and the Commissioner must consider the proportionality of the notice. Both must give the operator and the Secretary the opportunity to provide evidence, or make representations, to them before reaching their conclusions, which must be reported to the operator and the Secretary.
153 *IPB* cl 53.
154 *IPB* cl 59.
155 *IPB* cl 217.
156 *IPB* cl 217(5).
<table>
<thead>
<tr>
<th><strong>Communications-related data</strong></th>
<th><strong>General controls</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulk communications (meta) data</td>
<td>- Warrant only on application by head of intelligence service, subject to double-lock mechanism and a 6 month duration(^{157})</td>
</tr>
<tr>
<td>- Currently obtained under s 94 of Telecommunications Act 1984</td>
<td>- Foreign focused - warrant to be granted only where communications data which it is considered necessary to obtain relates to acts or intentions of persons outside the British Islands(^{158})</td>
</tr>
<tr>
<td></td>
<td>- Data may be selected for examination only so far as is necessary for the operational purposes specified in the warrant and selection must be necessary and proportionate(^{159})</td>
</tr>
<tr>
<td></td>
<td>- Data must be protected and access must be limited to the minimum that is necessary for the authorised purposes(^{160})</td>
</tr>
</tbody>
</table>

| Bulk equipment interference |  - Warrant only on application by head of intelligence service\(^{161}\), subject to double-lock mechanism\(^{162}\) and generally limited to a six month duration\(^{163}\) |
|  - Current use of powers avowed with the publication of the draft Equipment Interference Code of Practice in February 2015 |  - Must be foreign-focused and its main purpose must be to obtain data relating to overseas-related communications, equipment data or other data\(^{164}\) |
|  |  - May not examine content of persons in British Islands that may be contained within data\(^{165}\) without separate targeted examination warrant\(^{166}\) |
|  |  - Data may be selected for examination only so far as is necessary for the operational purposes specified in the warrant and selection must be necessary and proportionate\(^{167}\) |
|  |  - Data must be protected and access must be limited to the minimum that is necessary for the authorised purposes\(^{168}\) |

\(^{157}\) IPB cls 138 and 142.

\(^{158}\) IPB cl 138(3).

\(^{159}\) IPB cl 151

\(^{160}\) IPB cls 150 and 151(2).

\(^{161}\) IPB cl 91.

\(^{162}\) IPB cl 156 and 157.

\(^{163}\) IPB cl 162.

\(^{164}\) IPB cl 154.

\(^{165}\) IPB cl 170(4): ‘The prohibition referred to in subsection (3)(a) is that the protected material may not at any time be selected for examination if—
(a) any criteria used for the selection of the material for examination are referable to an individual known to be in the British Islands at that time, and
(b) the purpose of using those criteria is to identify protected material consisting of communications sent by, or intended for, that individual or private information relating to that individual. It does not matter for the purposes of this subsection whether the identity of the individual is known.’

\(^{166}\) IPB cl 88(9).

\(^{167}\) IPB cl 170.

\(^{168}\) IPB cls 168 and 169.
### Communications-related data

<table>
<thead>
<tr>
<th>Targeted equipment interference</th>
<th>Bulk interception</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A targeted equipment interference warrant is a warrant authorises a person to secure interference with reasonably described equipment, or equipment used by reasonably-described persons, for a reasonably-described purpose to obtain communications, equipment data, or any other information, including stored communications content, but does not entail interception.</td>
<td>• Current use under s 8(4) of RIPA held to be lawful and compliant with the ECHR by the IPT in Liberty &amp; Others</td>
</tr>
<tr>
<td>• Warrant application by head of intelligence service and issued only when necessary and proportionate</td>
<td>• Warrant only on application by head of intelligence service, subject to double-lock mechanism and generally limited to a six month duration.</td>
</tr>
<tr>
<td>• Separate but equivalent arrangements for warrants issued by Scottish Ministers in relation to Scotland and for Secretary to issue warrants on application by Chief of Defence Intelligence</td>
<td>• Must be foreign-focused and its main purpose must be to obtain data relating to overseas-related communications and secondary data from such communications.</td>
</tr>
<tr>
<td>• Law enforcement chief may similarly issue warrant in relation to law enforcement official but for criminal enforcement purposes only</td>
<td>• May not examine content of persons in British Islands that may be contained within data without separate targeted examination warrant.</td>
</tr>
<tr>
<td>• All these warrants are subject to double-lock mechanism and generally limited to a six month duration</td>
<td>• Data may be selected for examination only so far as is necessary for the operational purposes specified in the warrant and selection must be necessary and proportionate.</td>
</tr>
<tr>
<td></td>
<td>• Data must be protected and access must be limited to the minimum that is necessary for the authorised purposes.</td>
</tr>
</tbody>
</table>

---

169 IPB cl 101.

170 IPB cl 88(2).

172 IPB cls 92 and 93.

174 IPB cl 102.

175 IPB cls 121 and 123.

176 IPB cl 126.

177 IPB cl 119.

178 IPB cl 134(4).

179 IPB cl 13(3).

180 IPB cl 134.

181 IPB cls 132 and 133.
### Communications-related data

<table>
<thead>
<tr>
<th>Targeted interception</th>
<th>General controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Interception in the course of transmission</td>
<td>• Warrant only on application by heads of listed intelligence and law enforcement agencies, subject to double-lock mechanism and generally limited to a six month duration.</td>
</tr>
<tr>
<td></td>
<td>• Separate but equivalent arrangements for warrants issued by Scottish Ministers in relation to Scotland.</td>
</tr>
<tr>
<td></td>
<td>• Data must be protected and access must be limited to the minimum that is necessary for the authorised purposes.</td>
</tr>
</tbody>
</table>

### Bulk Personal Datasets (BPD)

| Large datasets with personal data of many individuals, most of whom are not, or are unlikely to be, of interest to intelligence agencies | Intelligence service may not examine a BPD retained by it unless examination is authorised by a class BPD warrant or a specific BPD warrant (naming the particular dataset) or another warrant or authorisation under the Act. |
| | Warrant only on application by head of intelligence service, subject to double-lock mechanism and generally limited to a six month duration. |
| | Data may be selected for examination only so far as is necessary for the operational purposes specified in the warrant and selection must be necessary and proportionate. |

### Summary and Implications

UK intelligence and law enforcement agencies enjoy extensive access to a wide range of government-held data, including non-clinical health data held by the NHS. Extensive criminal justice and vehicle data is centralised in databases such as the Police National Computer and supported by a number of advanced analytical capabilities. Automatic Number Plate Recognition (ANPR) technology is for example linked to the UK’s extensive CCTV network and provides automatic number plate recognition while CRIMELINK enables crime and intelligence analysts to identify patterns and links in crimes across the UK. The UK furthermore maintains various capabilities to access and mine social media.

---

182 IPB cl 16: the head of an intelligence service; the Director General of the National Crime Agency; the Commissioner of Police of the Metropolis; the Chief Constable of the Police Service of Northern Ireland; (e) the chief constable of the Police Service of Scotland; (f) the Commissioners for Her Majesty’s Revenue and Customs; (g) the Chief of Defence Intelligence; (h) a person who is the competent authority of a country or territory outside the United Kingdom for the purposes of an EU mutual assistance instrument or an international mutual assistance agreement.

183 IPB cl 21.

184 IPB cl 28.

185 IPB cls 19 and 20.

186 IPB cls 132 and 133

187 IPB cl 174(1).

188 IPB cl 175.

189 IPB cl 176 read with cl 192.

190 IPB cls 177-179.

191 IPB cl 184.

192 IPB cl 191.
The Investigatory Powers Bill will not dramatically increase the UK agencies’ access to data but will modernise, clarify and ensure greater consistency relating to, among others, the controls over and processes to access, retain, examine, exchange and delete private communications data. It will also increase overall transparency relating to these powers. A new requirement to keep internet connection records will add to the data that can be accessed under the Bill. The Bill does not regulate automatic data mining, only human examination of data.

3.2 Are legal controls comprehensive and proportional?

Access controls to communications data are set to change significantly under the regime envisaged by the Investigatory Powers Bill. However, it is important to consider the new Bill against the background of the current controls set out in RIPA.

3.2.1 RIPA

As discussed in 3.1.3, access to communications data under RIPA depends on the nature of the data. Communications (meta) data can be accessed on the strength of an authorisation issued by officials within the requesting agency while access to content data requires a warrant issued by a Secretary of State. Authorisation and warrants may only be issued if tests of necessity and proportionality are met, and processes may be inspected independent oversight bodies to ensure that appropriate tests were applied. While access controls are set to change under the Investigatory Powers Bill regime, the authorisation process will remain for less intrusive data access powers.

Warrants must comply with the Human Rights Act 1998 (UK) and article 8 of the European Convention on Human Rights. Article 8 provides as follows:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

In relation to the present regime, the ISC described the relevant test as a ‘triple test’, essentially combining legality, necessity and proportionality. Anderson described the challenges applying these tests to meet the interpretation of the European Court of Human Rights as follows:

5.19 The first element of that test is that the interference must be ‘in accordance with the law’. In other words:

(a) the interference must have some basis in domestic law;

(b) the law must be sufficiently accessible: the rules must be reasonably easy to obtain and understand; and

(c) the manner in which the law will operate or be applied must be sufficiently foreseeable.

5.20. These requirements have not always proved easy to reconcile with the secret nature of electronic surveillance. A balance must be found between retaining the secrecy of operational tools and methods on the one hand, and, on the other, having a law that is ‘sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities’ will access their communications.

5.21. The second element of the test involves the identification of a legitimate aim whose pursuit is necessary. Article 8(2) ... provides a broad list of interests that are capable of justifying interference. The courts are almost always willing to find that a legitimate aim is being pursued, for example, national security or the prevention of crime. ‘Necessary’ means...
less than ‘indispensable’, but more than merely ‘admissible’ or ‘useful’. To be necessary, an interference must correspond to a ‘pressing social need’.

5.22 To satisfy the third element of the test, the interference must be *proportionate* to the aim pursued. That is determined via a balancing exercise, which may for example require ‘the interest of the ... state in protecting its national security’ to be balanced against ‘the seriousness of the interference with the applicant’s right to respect for his private life’. The ECtHR [European Court of Human Rights] has repeatedly noted that:

(a) States have a ‘margin of appreciation’ (or, in the national court, a discretionary area of judgement). However, the court is the ultimate *arbiter of necessity*.

(b) In order to be satisfied that the interference is proportionate, courts must be satisfied that the national law sets out sufficient safeguards against abuse, and that those safeguards have been followed in the particular case (if appropriate).

29 The ISC described the UK statutory tests as follows:

The ‘triple test’ has been incorporated into various UK legislation, although the precise articulation varies. For example, Section 7 of the *Intelligence Services Act 1994* talks of Ministerial authorisation where action is for the ‘proper discharge of a function’, ‘necessary’ and ‘reasonable’; while RIPA uses slightly different wording, requiring a Secretary of State to assert that the conduct sought under a warrant is:

- ‘for a lawful purpose’ – for the Agencies this means it has to be in the interests of national security, to safeguard our economic well-being, or for the prevention and detection of serious crime;
- ‘necessary’ – i.e. the intrusion must be necessary for one of the purposes listed above; and
- ‘proportionate’ – i.e. the action must be no more intrusive than is justified for the purpose of the investigation, and must not unnecessarily intrude on the privacy of innocent people.

In determining whether it is necessary and proportionate, it must be considered whether the information could reasonably be obtained by other means.

The 2015 reports dealt with a variety of aspects relating to the warrant regime. This included whether warrants issued by a Secretary of State should rather be signed by judicial officers. The ISC advised against entrusting this responsibility to judges, maintaining that Ministers are able to consider the diplomatic and political context and not only the legal grounds and compliance:

The Agencies’ most intrusive capabilities are authorised by a warrant or other authorisation signed by a Secretary of State, with officials authorising those capabilities considered to be less intrusive. The primary question we have considered in this area is whether Ministers or judges should sign warrants for intrusive activity. We recognise the concerns put to us by some witnesses about public trust. However, the deciding factor for us is that while both Ministers and judges can assess legal compliance, Ministers can then apply an additional test in terms of the diplomatic and political context and the wider public interest. This additional test would be lost if responsibility were transferred to judges and might result in more warrant applications being authorised. Furthermore, judges are not held accountable, or asked to justify their decisions to Parliament and the public, as Ministers are. It is therefore


right that responsibility for authorising warrants for intrusive activity remains with Ministers ... 196

The Anderson report, on the other hand, was in favour of judges being granted this power: 197

All warrants should be judicially authorised by a Judicial Commissioner at a new body: the Independent Surveillance and Intelligence Commission (ISIC).

Where a warrant is said to be required in the interests of a national security purpose that relates to the defence and/or foreign policy of the UK, the Secretary of State should have the power so to certify (and, in the case of a bulk warrant, to certify that the warrant is required for the operation(s) or mission purpose(s) identified). The Judicial Commissioner, in determining whether to issue the warrant, should have the power to depart from that certificate only on the basis of the principles applicable in judicial review.

The Investigatory Powers Bill opted to increase judicial control over warrants while retaining political control. This is done by means of a so-called ‘double-lock’ system, discussed in 3.2.4–3.2.8.

3.2.2 Proportionality and analysis of data

Little public information is generally available about the operational controls that apply to the analysis of data for purposes of national security and law enforcement. However, in March 2016, Privacy International 198 gained access to redacted versions of formerly classified documents. These were released for purposes of the litigation and were published by Privacy International. 199 Extracts of GCHQ’s Compliance Guide, in force from June 2014 onwards, are of particular interest. These reflect the relevance of proportionality and necessity for purposes of analysis:

The individuals whose communications you examine have a right to privacy, so your work must conform to the standards of HRA. Your queries and analysis must be necessary for an intelligence requirement and proportionate. You usually have to demonstrate this through a HRA justification that is logged for audit.

If you are examining the content of individuals’ communications, the standard of your HRA justification must be higher than if you are examining events data. No additional authorisation is needed for querying and examining events data. 200

The principles are further detailed in a section entitled ‘Analyst responsibility’:

You are intruding on an individual’s right to privacy every time you search for their communications or communications about them in a database that contains raw traffic, or material derived from it. To conduct analysis in a way that is fully compliant with the law, every search that you carry out must be:

- authorised
- necessary for one of GCHQ’s purposes:
  - national security (NS)
  - economic well-being (EWB) of the UK (provided it also meets the NS Purpose)
  - prevention and detection of serious crime (SC)

---

198 The matter is before the Investigatory Powers Tribunal and focuses on the use by MI5, MI6 and GCHQ of s 94 powers. See <https://www.privacyinternational.org/node/854>.
• proportionate

To demonstrate the necessity and proportionality of your search, you must supply a HRA justification. ...\textsuperscript{201}

The Guide furthermore contains details regarding recording and logging of the HRA justification for each query of signal intelligence data by GCHQ users and audit and oversight processes. It also advises analysts to report legal non-compliance:

GCHQ policy is to abide by all UK laws that relate to GCHQ’s operations, but errors with respect to legal compliance, and to applying the safeguards do sometimes occur. This section outlines GCHQ’s process for handling errors and your role.

We need to be able to recognise and detect errors of legal compliance. We are obliged to investigate them and report to our oversight authorities.

If you have any concern over legal compliance or you identify an error that could breach GCHQ’s legal requirements or safeguards you should inform the relevant team straight away.

The relevant team will help and advise, if necessary coordinating GCHQ’s response.

GCHQ is happy to stand by those who make errors where they are inadvertent or otherwise explicable. The Department will not tolerate errors of a deliberate nature that seek to avoid or undermine the processes and systems by which GCHQ operates.\textsuperscript{202}

3.2.3 Data science ethical framework

While this discussion is focused on legal controls it is also important to note the emergence of ethical principles that would influence data analysts. A draft Data Science Ethical Framework was published by the Cabinet Office in December 2015.\textsuperscript{203} It was released as an early draft that was not yet government policy. The framework provides guidance for those working with data and persons making policy or operational decisions with data. The guidance is structured around six basic principles:

1. Start with a clear user need and public benefit: this will help you justify the level of data sensitivity and method you use.
2. Use the minimum level of data necessary to fulfil the public benefit: there are many techniques for doing so, such as de-identification, aggregation or querying against data.
3. Build robust data science models: the model is only as good as the data it contains and while machines are less biased than humans they can get it wrong. It’s critical to be clear about the confidence of the model and think through unintended consequences and biases contained within the data.
4. Be alert to public perceptions: put simply, what would a normal person on the street think about the project?
5. Be as open and accountable as possible: Transparency is the antiseptic for unethical behavior. Aim to be as open as possible (with explanations in plain English), although in certain public protection cases the ability to be transparent will be constrained.
6. Keep data safe and secure: this is not restricted to data science projects but we know that the public are most concerned about losing control of their data.\textsuperscript{204}

\textsuperscript{201} Privacy International, \textit{Extracts from GCHQ's Compliance Guide, in force from June 2014 onwards} (March 2016) 2.
\textsuperscript{204} Government Digital Service (UK), ‘Data Science ethics’ on \textit{Data in government} <https://data.blog.gov.uk/2015/12/08/data-science-ethics>.
These principles were not developed specifically for national security and law enforcement data experts, but if the framework hardens into government policy it is likely to extend to or at least influence intelligence and law enforcement analysts too.

3.2.4 Investigatory Powers Bill 2016: General framework

Provisions of the Investigatory Powers Bill include statutory controls on and oversight over access to and gathering of communications and bulk/large sets of data, its use and management by nine law enforcement and national security and intelligence agencies. The Bill consolidates and streamlines safeguards previously contained in several statutes including Regulation of Investigatory Powers Act 2000 (UK), Police Act 1997 (UK), Justice and Security Act 2013 (UK), Counter-Terrorism and Security Act 2015 (UK), and Data Retention and Investigatory Powers Act 2014 (UK). It also expands and re-shapes them.

At the heart of the proposed control system lies a new Investigatory Powers Commissioner and other Judicial Commissioners to be appointed under cl 194. These commissioners are discussed in 3.6 below. For purposes of this discussion it suffices to note that appointees must hold a judicial position of at least senior or a High Court judge.205 The IPC will replace the Interception of Communications Commissioner, the Chief Surveillance Commissioner and the Intelligence Services Commissioner.

In future, the warranty regime, the key control mechanism for the exercise of the most intrusive powers will operate on a double-lock system. This means that warrants must be ‘authorised by the Secretary of State and approved by a Judicial Commissioner’.206 While targeted equipment interference warrants for intelligence agencies and Defence will be subject to the double-lock system described below; warrants for law enforcement will be issued by a Chief Constable and a Judicial Commissioner.207

Less intrusive access powers will only require authorisations rather than warrants. The IPB allows designated senior officer of a relevant public authority to issue a targeted authorisation empowering officers of authority to access communication data if it is considered necessary and proportionate.208 The targeted access to communications data include ‘filtering arrangements’ established, controlled and maintained by the Secretary of State.

3.2.5 Investigatory Powers Bill: Secretary of State approval

Clause 17 of the Investigatory Powers Bill vests the power in the Secretary of State to issue personally209 three specific kinds of warrants on behalf of an ‘intercepting authority’,210 namely

205 Appointments of Judicial Commissioners will be made by the Prime Minister after consultation with the Lord Chief Justice of England and Wales, the Lord President of Scotland, the Lord Chief Justice of Northern Ireland, the Scottish Ministers, and the First Minister and deputy First Minister in Northern Ireland.


207 IPB cl 96.

208 IPB cl 53.

209 IPB cl 26 requires decisions to issue warrants to be taken personally by the Secretary of State.

210 IPB cl 16: ‘(1) Each of the following is an ‘intercepting authority’ for the purposes of this Part— (a) a person who is the head of an intelligence service; (b) the Director General of the National Crime Agency; (c) the Commissioner of Police of the Metropolis; (d) the Chief Constable of the Police Service of Northern Ireland; (e) the chief constable of the Police Service of Scotland [separate warranty regime]; (f) the Commissioners for Her Majesty’s Revenue and Customs; (g) the Chief of Defence Intelligence; (h) a person who is the competent authority of a country or territory outside the United Kingdom for the purposes of an EU mutual assistance instrument or an international mutual assistance agreement.’
targeted interception warrant, targeted examination warrant, and mutual assistance warrant. The Secretary of State must apply the test of ‘necessity’ and the test of ‘proportionality’.\(^{211}\)

It is apposite to note at this point that the IPB does not use ‘necessity’ and ‘proportionality’ but rather the adjectival terms ‘necessary’ and ‘proportionate’. As noted in by Anderson (see 3.2.1 above), the courts have construed the term ‘necessary’ in Article 8(2) of the European Convention on Human Rights as meaning less than ‘indispensable’, but more than merely ‘admissible’ or ‘useful’. To be necessary, an interference must correspond to a ‘pressing social need’.

The test of ‘proportionality’ refers to the ‘conduct authorised by the warrant … [which must be] proportionate to what is sought to be achieved by that conduct’. Clause 17(4) augments the proportionality test by requiring the Secretary of State to take into account ‘whether the information which it is considered necessary to obtain under the warrant could reasonably be obtained by other means.’

In addition, the Secretary of State must also consider whether additional statutory safeguards specific to the relevant targeted interception warrant, targeted examination warrant, and mutual assistance warrant have been fulfilled.\(^{212}\) These safeguards relate mainly to retention and disclosure of material.

Both the Secretary of State and Judicial Commissioners are bound by the statutory test of necessity in cl 18, which lists grounds that are applicable to each specific category of warrant. For example, cl 18(2) sets out the grounds for necessity in relation to targeted interception and examination warrants as follows:

A targeted interception warrant or targeted examination warrant is necessary on grounds falling within this section if it is necessary —

(a) in the interests of national security,

(b) for the purpose of preventing or detecting serious crime, or

(c) 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.

According to cl 18(3), a mutual assistance warrant\(^{213}\) is necessary on grounds falling within this section if—

(a) it is necessary for the purpose of giving effect to the provisions of an EU mutual assistance instrument or an international mutual assistance agreement, and

(b) the circumstances appear to the Secretary of State to be equivalent to those in which the Secretary of State would issue a warrant by virtue of subsection (2)(b). (i.e. for the purpose of preventing or detecting serious crime)

Clause 18(3)(b) provides an in-built ‘way out’ test to allow the Secretary of State to authorise warrants in circumstances unforeseen by the legislators. However, subsection 18(4) specifies that

\(^{211}\) IPB cl 17.

\(^{212}\) IPB cl 17(1)(c): ‘the Secretary of State considers that satisfactory arrangements made for the purposes of sections 46 and 47 (safeguards relating to disclosure etc) are in force in relation to the [targeted interception] warrant; cl 17(2)(c) ‘the Secretary of State that the [targeted examination] warrant is or may be necessary to authorise the selection of relevant content for examination in breach of the prohibition in section 134(4) (prohibition on seeking to identify communications of individuals in the British Islands)’; cl 17(3)(c) ‘the Secretary of State considers that satisfactory arrangements made for the purposes of sections 46 and 47 (safeguards relating to disclosure etc) are in force in relation to the [mutual assistance] warrant’.

\(^{213}\) Warrants made under the relevant mutual legal assistance treaty to which the United Kingdom is party for the purpose of gathering and exchanging information/data.
‘information which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands’ [i.e., it cannot pertain to people in Britain]. 214

The Secretary of State has full discretion to decide whether the cl 18 necessary warrant/conduct/measure is ‘proportionate to what is sought to be achieved by [it]’, in the sense that there are no mandated statutory factors to be taken into account. This means that the Secretary of State can use his/her political judgment; though in cases of mutual assistance, he/she would also refer to the EU test of proportionality. These two tests are supplemented by a procedural requirement that ‘except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant must be approved by a Judicial Commissioner’. Such warrants may only be issued in a limited number of serious cases and the decision to issue the urgent warrant is subject must be reviewed by a Judicial Commissioner within three days.215

In relation to the two tests, IPB complicates matters by mandating the Secretary of State to ‘ensure’ [‘must ensure’], inter alia, that a different statutory test of necessity and proportionality, is applied by ‘senior officers’216 in the context of safeguards relating to examination217 (retention and destruction) of:

- the content and secondary data obtained under interception warrants (cl 134(1)(b));
- communication data obtained under bulk interception warrants (cl 151(1)(b)),
- data obtained under bulk equipment interference warrant (cl 170 (1)(b));
- and datasets obtained under bulk personal data interception warrants (cl 191(1)(b)).

This test states that:

‘the selection of any of [the intercepted content, secondary data, communication data, data, material, etc] for examination is necessary and proportionate in all the circumstances’.

The test is directed at the personnel handling the acquired data, and ensures that the principles of necessity and proportionality are systemically embedded in the legislation, albeit in different forms.

At this level, the ‘necessity’ test has different terms of reference: ‘in all the circumstances’ implying capacity to include considerations that cannot be defined in advance.

3.2.6 Investigatory Powers Bill: Judicial Commissioner approval

The second part of the ‘double-lock system’ involves the Judicial Commissioners’ power to approve warrants under cl 21 of the Investigatory Powers Bill 2016.218

---

214 In relation to Australia, the Intelligence Services Act 2001 (Cth) s 13A authorises ASIS, AGO and ASD to cooperate with intelligence agencies, ASIO, and Commonwealth and State authorities in connection with performance of their functions. These agencies are bound by the Guidelines to Protect Privacy of Australian Persons <http://www.defence.gov.au/dio/privacy-rules.shtml>. Principle 1.1 of the Guidelines states: ‘These rules regulate the communication and retention of Australian persons. Where it is not clear whether a person is an Australian person, the following presumptions shall apply unless there is evidence to the contrary including from the context in which the intelligence was obtained:

a. a person within Australia shall be presumed to be an Australian person, and
b. a person outside Australia shall be presumed to not be an Australian person.’

215 IPB cl 22(3).

216 IPB cls 134(7), 151(7), 170(7), 191(7) define ‘senior officer’, as ‘a member of the intelligence service who—(a) is a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty’s Diplomatic Service, or (b) holds a position in the intelligence service of equivalent seniority to such a member’.

217 IPB cl 225(7) defines examination for purposes of the Act as ‘the examination of material obtained under a warrant are references to the material being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant.’ ‘the examination of material obtained under a warrant’ as ‘the material being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant’.

218 Notably, Judicial Commissioners have the power to approve both, warrants issued by the Secretary of State and those issued by Scottish Ministers under cl 19 of the IPB.
In general, all provisions involving authorisations by the Secretary of State acknowledge that, subject to the statutory necessity test, these are ultimately policy decisions. The proportionality notion is included because of its pivotal role in the approval of the authorised warrant under the ‘double-lock system’ by Judicial Commissioners. While Judicial Commissioners must apply the cl 18 necessity test already applied by the Secretary of State, their determination regarding the proportionality criterion must be in the form of legal review, presumably based on the common law test of proportionality.

A Judicial Commissioner must review the person’s conclusions regarding the following –

(a) whether the warrant is necessary on the relevant grounds, namely targeted interception warrant, targeted examination warrant, and mutual assistance warrant as set out in cl 18 (discussed above), and
(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

3.2.7 Investigatory Powers Bill: Complexity in the double lock system

While both the Secretary and the Judicial Commissioner must consider whether the proposed conduct that would be authorised by the warrant is proportionate to what is sought to be achieved, the Act does not provide the test for proportionality to be applied by each of them, except mandating in cl 21 (2) that:

in doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.219

Jurisprudence of the proportionality principle in England is exceedingly complex.220 Broadly, the English common law principle of proportionality differs from the general principle of proportionality contained in the Treaty on European Union,221 and the applicability of each is context-dependant. Also context-dependant is the strictness with which the EU proportionality law is construed.

At the EU level, Article 5(4) of the Treaty on European Union states that:

Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.

According to the Supreme Court of England and Wales, the EU general principle of proportionality involves ‘a consideration of two questions: first, whether the measure in question is suitable or appropriate to achieve the objective pursued; and secondly, whether the measure is necessary to achieve that objective, or whether it could be attained by a less onerous method.’222

---

219 There are two procedural control mechanisms: IPB cl 21(4) requires the Judicial Commissioner who refuses to approve a person’s decision to issue a warrant to provide written reasons for the refusal; and cl 21(5) provides that where ‘a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a person’s decision to issue a warrant …, the person may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant’.


221 Bank Mellat [2013] UKSC 39, [2013] 3 WLR 179, [69] (Lord Reed); see also Nicklinson [2014] UKSC 38; [2015] 1 AC 657, [169] (Lord Mance). Article 6 TEU provides that the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union ‘shall have the same legal value as the Treaties’, and that the ‘Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms’.

This principle applies, inter alia, ‘to national measures falling within the scope of EU law’, which interfere with protected interests including the fundamental freedoms guaranteed by the EU Treaties. As mentioned above, mutual assistance warrants are issued pursuant to EU’s Agreement with the United States on mutual legal assistance. Once enacted, the validity of the Investigatory Powers Act 2016 might be challenged, for example, on the ground that it infringes the EU principle of proportionality because its controls provide inadequate safeguards against interference with fundamental freedoms guaranteed by the EU Treaties. However, given that the Investigatory Powers Act 2016 is a national measure, the matter would be determined by the national court through application of the ‘two question’ test (and the jurisprudence of the European Court of Justice). Indeed, the Investigatory Powers Bill, cl 208 creates a domestic right of appeal from decisions or determinations of the IPT to the Court of Appeal in England and Wales, the Court of Session or the Court of Appeal in Northern Ireland.

To make matters more complex, ‘the principle of proportionality in EU law is neither expressed nor applied in the same way as the principle of proportionality under the European Convention on Human Rights’. The latter principle has become part of the English common law jurisprudence. Articulated by Dickson CJ in R v Oakes [1986] 1 SCR 103, the principle of proportionality was adopted and developed further by the House of Lords, and provides: a four-stage analysis of proportionality in relation to the justification under domestic law (in particular, under the Human Rights Act 1998 [UK]) of interferences with fundamental rights.

In Bank Mellat v HM Treasury (No 2) [2013] UKSC 39; [2013] 3 WLR 179 at [74], Lord Reed thus summarised the four questions to be considered under the English principle of proportionality:

‘(1) whether the objective of the measure is sufficiently important to justify the limitation of a protected right, (2) whether the measure is rationally connected to the objective, (3) whether a less intrusive measure could have been used without unacceptably compromising the achievement of the objective, and (4) whether, balancing the severity of the measure’s effects on the rights of the persons to whom it applies against the importance of the

---

223 Lumsdon [2015] UKSC 41; [2015] 3 WLR 121, [29] (Lord Reed and Lord Toulson). The EU principle of proportionality is context-dependant: it is construed less strictly in cases concerning measures that implement EU legislation by member states, and more strictly ‘where member states rely on reservations or derogations in EU legislation in order to introduce measures restricting fundamental freedoms …’ [38].

224 Lumsdon [2015] UKSC 41; [2015] 3 WLR 121, [73] (Lord Reed and Lord Toulson).

225 Lumsdon [2015] UKSC 41; [2015] 3 WLR 121, [25] (Lord Reed and Lord Toulson). Article 2 of the Treaty on European Union (TEU) provides that ‘the Union is based on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities’.


227 Lumsdon [2015] UKSC 41; [2015] 3 WLR 121, [23] and [31] (Lord Reed and Lord Toulson) (Lord Neuberger, Lady Hale and Lord Clarke agreeing).

228 The appeals can be heard wholly or partly in closed material proceedings, if it is necessary for the appeal court to review information which was considered by the Investigatory Powers Tribunal in closed session.


232 Lord Sumption, Lady Hale, Lord Kerr and Lord Clarke agreeing at [20]; Lord Neuberger agreeing at [166].
objective, to the extent that the measure will contribute to its achievement, the former outweighs the latter.\textsuperscript{233}

These, very carefully worded, criteria that comprise the principle of proportionality are applicable across all relevant contexts,\textsuperscript{234} and presumably would be applied under cl 21 by the Judicial Commissioners when determining whether the agency’s authorised warrant should be approved. However, in \textit{Bank Mellat v HM Treasury} (No 2) [2013] UKSC 39, [2013] 3 WLR 179, at [71],\textsuperscript{235} Lord Reed also cautioned that:

An assessment of proportionality inevitably involves a value judgment at the stage at which a balance has to be struck between the importance of the objective pursued and the value of the right intruded upon. The principle does not however entitle the courts simply to substitute their own assessment for that of the decision-maker.

The question therefore arises whether Judicial Commissioners in applying ‘the same principles as would be applied by a court on an application for judicial review’ mandated by cl 21(2), have the role of a ‘court’ or do they remain ‘decision-makers’ vested with the power of approval.

3.2.8 Investigatory Powers Bill: Application of the double-lock mechanism

The double-lock mechanism applies to approval of all warrants involving:

1. Equipment interference, ‘normal’, urgent, and renewal of warrants [cl 97, 98, and 103],\textsuperscript{236} (their issuance must be \textit{necessary in the interests of national security});\textsuperscript{237}
2. Bulk interception warrants: approval of warrants by Judicial Commissioners, renewal, modifications, approval of modifications to warrants in urgent cases [cl 123, 127, 128, 129];
3. Bulk acquisition warrants: approval of warrants by Judicial Commissioners, renewal, modification, approval of major modifications made in urgent cases [cl 139, 143, 144, 145];
4. Bulk equipment interference warrants: approval of warrants by Judicial Commissioners, approval of warrants issued in urgent cases, renewal of warrants; modification of warrants, approval of major modifications made in urgent cases [cl 157, 158, 163, 164, 165];
5. Bulk Personal Dataset Warrants (Class BPD warrants, cl 177 and Specific BPD warrants, cl 178 involve large datasets containing personal information about a wide range of people): approval of warrants by Judicial Commissioners, approval of specific BPD warrants issued in urgent cases, renewal of warrants, modification of warrants, approval of major modifications made in urgent cases [cl 179, 180; 185, 186, 187].

3.2.9 Investigatory Powers Bill: Other access control mechanisms

Controls are not limited to the double-lock system.

\textsuperscript{233} The formulation of Lord Sumption in \textit{Bank Mellat} 3 WLR 170, [2013] UKSC 39, [20], which adds ‘a fair balance has been struck between the rights of the individual and the interests of the community’ requirement has been cogently criticised in \textit{Miranda} [2014] EWHC 255 (Admin); [2014] HLR 9; [2014] 1 WLR 3140, [40] by Lord Justice Laws MR (Ouseley and Openshaw JJ in agreement).


\textsuperscript{235} Lord Sumption, Lady Hale, Lord Kerr and Lord Clarke agreeing at [20]; Lord Neuberger agreeing at [166].

\textsuperscript{236} To access data from computers, smartphones etc. by the security and intelligence agencies, law enforcement and the armed forces.

\textsuperscript{237} The new \textit{Draft Code of Practice on Equipment Interference} for the security and intelligence agencies identifies the following objectives:

\begin{itemize}
  \item [a)] obtain information from the equipment in pursuit of intelligence requirements;
  \item [b)] obtain information concerning the ownership, nature and use of the equipment with a view to meeting intelligence requirements;
  \item [c)] locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in (a) and (b);
  \item [d)] enable and facilitate surveillance activity by means of the equipment;
  \item ‘Information’ may include communications content, and communications data.’
\end{itemize}
Although the provisions of the Investigatory Powers Bill are intended for Agency personnel at the very high level of decision-making, some analysts would also be covered by other control measures including those in the form of safeguards relating to retention and disclosure that attach to the interception of communication data, equipment interference warrants. In these cases, the 'issuing authority' must ensure, in relation to each targeted interception warrant, mutual assistance warrant, or targeted equipment interference warrant that:

arrangements are in force for securing ... in relation to the material obtained under a warrant ... [that] each of the following is limited to the minimum that is necessary for the authorised purposes: (a) the number of persons to whom any of the material is disclosed or otherwise made available; (b) the extent to which any of the material is disclosed or otherwise made available; (c) the extent to which any of the material is copied; (d) the number of copies that are made.

Essentially the same controls apply to bulk interception warrants, bulk acquisition warrants, bulk equipment interference warrants, and bulk personal dataset warrants; however, in these cases, the Secretary of State is under duty to ensure that appropriate arrangements are in place. As a general rule, every copy made of any of the material acquired under warrant must be destroyed ‘as soon as there are no longer any relevant grounds for retaining it’.

Supplementary controls provide safeguards for examination of the intercepted content and secondary data obtained under bulk interception warrants, bulk acquisition warrants, bulk equipment interference warrants and bulk personal dataset warrants by mandating that:

(a) any selection of data, the intercepted content, secondary data, bulk personal datasets, for examination is carried out only for the specified purposes; (b) the selection of any of the data for examination is necessary and proportionate in all the circumstances, and (c) the selection of any of the intercepted content for examination meets any of the statutory selection conditions.

238 IPB cl 16: ‘Persons who may apply for issue of a warrant
(1) Each of the following is an ‘intercepting authority’ for the purposes of this Part—
(a) a person who is the head of an intelligence service;
(b) the Director General of the National Crime Agency; (c) the Commissioner of Police of the Metropolis;
(d) the Chief Constable of the Police Service of Northern Ireland;
(e) the chief constable of the Police Service of Scotland;
(f) the Commissioners for Her Majesty's Revenue and Customs;
(g) the Chief of Defence Intelligence;
(h) a person who is the competent authority of a country or territory outside the United Kingdom for the purposes of an EU mutual assistance instrument or an international mutual assistance agreement.’

239 IPB cls 16 and 17 provide safeguards relating to disclosure of material overseas.

240 IPB cls 112 and 113.
241 IPB cls 132 and 133.
242 IPB cls 150 and 151.
243 IPB cls 168 and 169.
244 IPB cls 191 and 192
245 In the case of bulk interception warrants, ‘intercepted content or secondary data’.

246 IPB cl 134.
247 IPB cl 151.
248 IPB cl 170.
249 IPB cl 191: ‘(1) The Secretary of State must ensure, in relation to every class BPD warrant or specific BPD warrant which authorises examination of bulk personal datasets of a class described in the warrant or (as the case may be) of a bulk personal dataset described in the warrant, that—(a) any selection of data contained in the datasets (or dataset) for examination is carried out only for the specified purposes, and (b) the selection of any such data for examination is necessary and proportionate in all the circumstances. (2) The selection of data contained in bulk personal datasets for examination is carried out only for the specified purposes if the data is selected for examination only so far as is necessary for the operational purposes specified in the warrant in accordance with section 183.’
Another form of control involves duty not to make unauthorised disclosures. This duty is imposed in relation to interception, equipment interference warrants, bulk interception warrants, and bulk equipment interference warrants.

3.2.10 Investigatory Powers Bill: Offences

As part of measures to safeguard privacy, the IPB introduced offences for (a) the unlawful interception of communications, and (b) the unlawful obtaining of communications data. These are set out in Part 1, cl 2(1), which makes it an offence to:

intentionally intercept, in the United Kingdom, a communication in the course of its transmission, without lawful authority.

However it is not criminal offence for a person to use computer networks in the home or workplace, if he/she has the right to control the operation or use of the system or has the expressed or implied consent of such a person to carry out the interception (cl 2(2)). Clause 3, subsections (1) and (2) provide that persons intercept telecommunications system communications if:

(a) they make some or all of the content of a communication available to a person who is not the sender or intended recipient; (b) modify or interfere with the system; (c) monitor transmissions made by means of the system or monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system.

Under cl 3(4)(b), a communication is still regarded as being in the course of its transmission when it is stored in or by the system used to transmit it. A stored communication includes communications stored on phones, tablets and other individual devices whether before or after its transmission.

---

250 IPB cl 49 imposes a duty not to make unauthorised disclosures on ‘(a) any person who is an intercepting authority (see section 16); (b) any person holding office under the Crown; (c) any person employed by, or for the purposes of, a police force; (d) any postal operator or telecommunications operator; (e) any person employed or engaged for the purposes of the business of a postal operator or telecommunications operator; (f) any person to whom any of the matters within subsection (4) have been disclosed in relation to a warrant.’

251 IPB cl 114 imposes a duty not to make unauthorised disclosures on ‘(a) any person who may apply for a warrant...; (b) any person holding office under the Crown; (c) any person employed by, or for the purposes of, a police force; (d) any telecommunications operator; (e) any person employed or engaged for the purposes of any business of a telecommunications operator; (f) any person to whom any of the matters within subsection (4) have been disclosed in relation to [equipment interference] warrant.’

252 IPB cl 136(2): ‘Sections 49 to 51 (duty not to make unauthorised disclosures) apply in relation to bulk interception warrants as they apply in relation to targeted interception warrants, but as if the reference in section 50(2)(c) to a requirement for disclosure imposed by virtue of section 109(4) were a reference to such a requirement imposed by virtue of section 131(4).’

253 IPB cl 172: ‘Sections 114 to 116 (duty not to make unauthorised disclosures) apply in relation to bulk equipment interference warrants as they apply in relation to targeted equipment interference warrants, but as if the reference in section 115(2)(c) to a requirement for disclosure imposed by virtue of section 109(4) were a reference to such a requirement imposed by virtue of section 167(4).’

254 Communication includes: communications in the course of transmission on a public telecommunications system (the hardware and software used to provide a telecommunications service to the public in the United Kingdom); private telecommunications system (separate from, but connected to a public telecommunications system, includes computer networks in the home or workplace); or a public postal service.

255 IPB cl 221(4) amends the Wireless Telegraphy Act 2006 (UK), s 48 (interception and disclosure of messages) to read: [s 48] ‘(3A) A person does not commit an offence under this section consisting in any conduct—(a) constitutes an offence under section 2 of the Investigatory Powers Act 2016 (offence of unlawful interception), or (b) would do so in the absence of any lawful authority (within the meaning of section 5 of that Act).’

256 Under IPB cl 2(6), the Investigatory Powers Commissioner may impose a fine (must not exceed £50,000) on a person who is found guilty of the offence of unlawful interception under cl 2(1); such person may be convicted on indictment for a maximum of two years’ imprisonment; or be fined and imprisoned.
Clause 9(1) creates the offence of knowingly or recklessly, without lawful authority, obtaining communications data from a telecommunications or postal operator. The offence is directed at persons within a public authority/agency with powers to acquire communications data under Part 3 of the Bill. However, it is a defence to act under the reasonable belief of having a lawful authority to obtain the communications data.

Clause 51 creates the offence of failure to comply with the duty of non-disclosure relating to targeted interception warrant. Clause 49(4) provides that unless authorised, the duty of non-disclosure encompasses:

(a) the existence or contents of the warrant; (b) the details of the issue of the warrant or of any renewal or modification of the warrant; (c) the existence or contents of any requirement to provide assistance in giving effect to the warrant; (d) the steps taken in pursuance of the warrant or of any such requirement; (e) any of the material obtained under the warrant.\textsuperscript{257}

In relation to targeted authorisations, cl 73(1) creates the offence for:

a telecommunications operator, or any person employed or engaged for the purposes of the business of a telecommunications operator, to disclose, without reasonable excuse, to any person the existence of— (a) any requirement imposed on the operator by virtue of this Part to disclose communications data relating to that person, or (b) any request made in pursuance of an authorisation for the operator to disclose such data.\textsuperscript{258}

Clause 116 creates an offence of making unauthorised disclosure under targeted equipment interference warrants and targeted examination warrants in relation to:

(a) the existence or contents of the warrant; 
(b) the details of the issue of the warrant or of any renewal or modification of the warrant; 
(c) the existence or contents of any requirement to provide assistance in giving effect to the warrant; 
(d) the steps taken in pursuance of the warrant or of any such requirement; 
(e) any of the material obtained under the warrant in a form which identifies it as having been obtained under a warrant under this Part (cl 114(4)).\textsuperscript{259}

An offence of making unauthorised disclosure in relation to bulk acquisition warrants is created under cl 152(1), which provides that it is an offence for

(a) a telecommunications operator who is under a duty by virtue of section 149 to assist in giving effect to a bulk acquisition warrant, or 
(b) any person employed or engaged for the purposes of the business of such an operator, to disclose to any person, without reasonable excuse, the existence or contents of the warrant’.\textsuperscript{260}

\textsuperscript{257} Defence: cl 51(3): ‘(3) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the person could not reasonably have been expected, after first becoming aware of the matter disclosed, to take steps to prevent the disclosure’.

\textsuperscript{258} Reasonable excuse: cl 73 ‘if the disclosure is made with the permission of the relevant public authority which is seeking to obtain the data from the operator (whether the permission is contained in any notice requiring the operator to disclose the data or otherwise)’.

\textsuperscript{259} Defence: cl 115(3): ‘if the person could not reasonably have been expected, after first becoming aware of the matter disclosed, to take steps to prevent the disclosure’.

\textsuperscript{260} IPB cl 154(6) provides that ‘A bulk equipment interference warrant may not, … authorise a person to engage in conduct, in relation to a communication other than a stored communication, which would (unless done with lawful authority) constitute an offence under section 2(1) (unlawful interception)’.
Apart from offences relating to unlawful disclosures, by virtue of cl 35(7), it is an offence for the relevant operator to knowingly fail to assist with implementation of targeted interception warrants and mutual assistance warrants (under cl 34) by (or on behalf of) the intercepting authority.

Offences for the breach of non-disclosure provisions include imprisonment for a term not exceeding 12 months on summary conviction or fine in England and Wales (with different provisions for Scotland and the Northern Ireland).261

3.2.11 Investigatory Powers Bill: Special controls for ‘sensitive professions’

The IPB privileges certain groups within the UK. Thus, cl 24 introduces additional controls by requiring the Secretary of State to consult the Prime Minister before issuing targeted and examination warrants to intercept communications of a person who is a Member of Parliament, a Member of the European Parliament representing the United Kingdom, or a member of one of the devolved legislatures.

Clause 25262 provides that where the purpose, or one of the purposes of a warrant (targeted interception warrant, mutual assistance warrant or targeted examination warrant)263 is to obtain communications subject to legal privilege, the warrant application must contain a statement, and the person authorising the warrant must be satisfied:

a. ‘that there are exceptional and compelling circumstances that make it necessary to authorise the interception, or (in the case of a targeted examination warrant) the selection for examination’, and

b. that specific arrangements are in place for the handling, retention, use and destruction of ‘items subject to legal privilege’, which include communications between a lawyer and their client, or a person representing that client, in connection with legal advice or legal proceedings.264

In addition, sources of journalistic information were protected by the requirement under cl 53 that targeted authorisations for obtaining communications data to identify or confirm such sources are subject to approval by the Judicial Commissioner (cl 68).

While the improvement were acknowledged, the UK government faced political pressure to make further changes to enhance protection of journalistic sources, improve protection of legal privilege and ensuring Prime Ministerial sign-off on warrants involving members of Parliament.265

---

261 IPB cls 51, 116 and 152.
262 In conjunction with the Home Office (UK), Interception of Communications Code of Practice (archived April 2014) ch 9.
263 There are equivalent provisions in relation to equipment interference warrants, bulk interception and acquisition warrants, bulk equipment interference warrants, and bulk personal dataset warrants.
264 See also IPB cl 29 with special provisions for renewal of warrants issued under cl 24 and cl 25; cl 30 which contains special provisions for modifications of such warrants; and cl 46, which requires that ‘the Investigatory Powers Commissioner must be informed where material subject to legal privilege is retained’
265 See 1.3.3.
Summary and Implications

Under the current regime, metadata can be accessed on the strength of an authorisation issued by senior officials within the requesting agency while access to content data requires a warrant issued by a minister. Authorisation and warrants may only be issued if tests of lawfulness, necessity and proportionality are met, and processes may be inspected by independent oversight bodies to ensure that appropriate tests were applied. The three 2015 reports (RUSI, Anderson and ISC) found that the legal framework regarding access to and retention, examination, exchange and deletion of private communications data is out-dated and lacking in public trust. The Investigatory Powers Bill was therefore introduced with stated objective to improve control measures by increasing their clarity and consistency. In particular, the Bill provides data-specific rather than agency-specific rules for data. Data in turn is differentiated on the strength of the characteristics of the data-set in question (bulk, interference with equipment, etc.), and the nature of usage (access, sharing, retention, etc).

The Bill retains the important tests of lawfulness, necessity and proportionality but introduces judicial review for the exercise of the most intrusive powers by means of a so-called double-lock system. This system is embedded in warranty procedures that have been streamlined and standardised. The Bill also enhances oversight and transparency to improve public trust in the operation of the system.

The powers under the Bill, especially powers to access and retain bulk data sets and the obligation to keep Internet Connection Records (see 3.1.5) are controversial and concerns have been raised regarding compliance with the laws of the EU. As discussed in 1.3.3 the UK government has met with political and civil society pressure to restrict the powers and increased the protection of privacy. Some concessions may be made and the government also announced that the Independent Reviewer of Terrorism Legislation will review the proposed surveillance powers under the Bill.

3.3 Are legal rules clear, principle-based, consistent and instructive?

The third line of enquiry focuses on some of the attributes of the current UK laws and regulations relevant to Big Data and national security. It responds to the third Lens item by considering whether the framework is expressed in clear, principle-based and consistent legal rules that provide officials with appropriate guidance to take reasonable decisions and perform their functions correctly and efficiently in a dynamic environment.

The access and control framework as described in 3.1 and 3.2 is complex. It was not possible to determine in this study whether these laws and regulations are sufficiently clear to provide officials with appropriate guidance. In particular, much of the guidance on the application of current laws is contained in confidential internal policies and manuals that the researchers could not review. Many of the operational details regarding the IPB, on the other hand, will only be produced once the Bill has been adopted.

Compliance audits done by independent oversight bodies provide a measure of comfort that compliance levels are high (see 3.6). By implication, it would therefore be reasonable to assume that the internal policies and operational rules are sufficiently clear to prevent non-compliance. It is less clear whether they are sufficiently clear to enable officials to act confidently within the full scope of what the law allows.

---

266 See, e.g., Anthony May in Interception of Communications Commissioner’s Office, Report of the Interception of Communications Commissioner House of Commons Paper 1113, Session 2014-15 (March 2015) 2: ‘[The Commissioner’s] office has continued to undertake our audits of public authorities’ use of these intrusive powers against existing legislation and to make recommendations to improve compliance. Overall the inspections carried out by my office show that the staff within the public authorities have a desire to comply with the legislation and to achieve high standards in the work that they carry out. There is a strong culture of compliance and of self-reporting when things go wrong.’
3.3.1 Clarity and flexibility of the current laws

Legal clarity was rated as very important by all three 2015 reviews and its absence noted in relation to the current, that is the pre-Investigatory Powers Bill regime:

There is no one piece of legislation that governs what the intelligence and security Agencies can and cannot do: broadly, the Security Service Act 1989 and the Intelligence Services Act 1994 provide the legal basis for the Agencies’ activities, but that is subject to the overarching requirements of the Human Rights Act 1998, and further constraints on certain of those activities as set out in a number of other pieces of legislation (for example, the Regulation of Investigatory Powers Act 2000). This is not just opaque, it is unnecessarily complicated. Further, it is inappropriate that many key capabilities – for example, the exchange of intelligence with international partners – are implicitly authorised rather than formally defined in statute.267

In addition, the secret parts of the state have operated under domestic legal conditions of great complexity, where law has been accumulated into a regime that has baffled legal professionals and practitioners alike. This is not a sound basis on which to confront the technological and democratic challenges of the future. The legal expression of state powers should never be a thing of shreds and patches. Legislative clarity is not merely a matter of presentation in the business of interception and surveillance; it is fundamental to democracy.268

Investigatory powers and practices often involve secret, or covert, actions. The importance of coherence and clarity, a desirable feature in any area of the law, is heightened in this context. Unfortunately, however, RIPA itself is complex, fragmented and opaque. It is extraordinarily difficult both to understand and to apply.269

The Anderson review also quoted from the submission Liberty made to it, stating that ‘a striking feature of RIPA is that it treats the various forms of surveillance in a patchy and inconsistent manner’.270

Statutory terminology was also identified as problematic. In relation to RIPA for example it was observed that important concepts such as ‘content’ were not defined271 and the definitions of terms such as ‘communications’ (especially ‘external communications’, and ‘internal communications’),272 and ‘subscriber data’ were anachronistic and counter-intuitive.273

Confusion is compounded by the fact that many rules in the legislation and accompanying Codes of Practice are insufficiently detailed.274 RUSI commented that the lack of clarity extends to the powers and safeguards governing the exchange of data and intelligence between international partners.275

Internal legal interpretations of RIPA also play an important role. The fact that agencies interpreted section 8 of RIPA to allow for the issuing of thematic warrants was, for example, not publicly known until this interpretation was first avowed in the ISC’s Privacy and Security Report in March 2015.276
What was therefore thought to be clear publicly about the ambit of section 8, was not the case.

---

3.3.2 Clarity, flexibility and the Investigatory Powers Bill 2015

The Investigatory Powers Bill was drafted with the objective to clarify the law. Appropriate terminology was formulated (see Chapter 1 and 3.2) and consistency of rules and procedures was promoted to assist in the administration of the Act and the powers under the Act.

Parliamentary Committees that considered the draft Bill believed that more could be done to clarify and law. The Joint Parliamentary Committee, for example, addressed various concerns relating to a lack of clarity. It recommended for example that key concepts such as ‘national security’ and ‘economic well-being’, the grounds on which warrants to access communication-related data can be exercised (see 3.2), should be clarified:

(690). Witnesses have pointed out that the term ‘national security’, which can be used to justify so many of the actions provided for in the draft Bill, is never defined anywhere in the Bill. Rachel Logan from Amnesty International UK said, ‘just recently, a decision by the Grand Chamber in Strasbourg, I think last week, said that it is important to have tighter definitions than just ‘threats to national security when we talk about warrants of this kind.’

(691). The Committee recommends that the Bill should include a definition of national security in order to provide clarity to the circumstances in which these warrants can be issued. (Recommendation 82)...

(695). The UN Special Rapporteurs were concerned that ‘ambiguous terms such as ‘economic well-being’, [heighten] the risk of excessive and disproportionate interception.’

(696). The Committee recommends that the Bill should include a definition of economic well-being in order to provide clarity to the circumstances in which these warrants can be issued. (Recommendation 83)

While the government responded to recommendations of the parliamentary committees, it did not adopt these recommendations and responded as follows:

It has been the policy of successive governments not to define national security in statute. Threats to national security are constantly evolving and difficult to predict, and it is vital that legislation should not constrain the ability of the security and intelligence agencies to protect the UK from new and emerging threats.

The Bill provides for warrants to be sought in the interests of the economic-well-being of the United Kingdom so far as also relevant to national security. This replicates the current statutory purpose for which interception warrants may be authorised and which is contained in RIPA, replicates language in the e-privacy directive, and is consistent with the statutory functions of GCHQ and the Secret Intelligence Service. The ‘economic well-being’ purpose for which warrants may be sought is not precisely identical to the ‘national security’ purpose. Consequently, removing ‘economic well-being’ from the Bill could have the effect of preventing the agencies from undertaking operations in future that they would be able to undertake today. The UK’s National Security Strategy and Strategic Defence and Security Review 2015 highlighted economic security as a separate issue that is closely related to national security, and reflected the long-term shifts in the balance of global economic and military power and the emergence of more powerful non-state actors. It would not be appropriate to hinder the ability of the security and intelligence agencies to undertake investigative activity into issues where the primary risk is to economic security, which has an effect on national security. Such issues might include instability in parts of the world or unexpected crises which may undermine British markets and other economic interests, or create difficulties in the continued supply of a commodity on which our economic security...

publicly avowed only on 12 March 2015 when the ISC published its report. I had already been extensively briefed on their use at all three agencies, and was also aware that the ISCommr has, for several years, been reviewing the use of bulk personal datasets as part of his duties.’

depended. Such issues would also have a national security impact but their primary effect could be on economic well-being.²⁷⁸

While the Investigatory Powers Bill 2016 therefore clarifies very important concepts, some key concepts still remain undefined with the specific objective not to hinder security and intelligence agencies in their application of powers under the Act as circumstances evolve.

Summary and Implications

There is general agreement that the current regime enabling access to telecommunications data and its retention, analysis, sharing and destruction is unclear and inconsistent. In addition the terminology and processes have not kept up with technological developments. The lack of clarity provides room for confusion and undermines public trust in the system. The Investigatory Powers Bill was therefore drafted in order to clarify the law. Improved terminology was formulated (see Chapter 1 and 3.2) and consistency of rules and procedures was promoted that will assist in the administration of the Act and the powers under the Act.

The Investigatory Powers Bill 2016 employs improved terminology reflecting current technological concepts. It standardises authorisation and warranty processes and improves overall consistency in relation to control and oversight measures. Different groups hold different views about the level of clarity of some of the terms and measures, but, given the complexity of the subject matter and the range of issues to be addressed, perfect clarity and simplicity are likely to remain elusive.

3.4 Is integrity of data and analysis supported?

The fourth line of enquiry addresses the need for data quality and integrity as well the integrity of the inferences drawn from data through analysis and employed in decision-taking. This section considers current rules that would support the integrity of data collected, retained and accessed by government for law enforcement and national security purposes, and the integrity of analytical and decision-making uses of such data and systems.

At the most basic level, integrity of data and information in this field requires retaining metadata, referred to in the IPB as ‘secondary data’ about its provenance. This means retaining information on its source, the probability that it contains errors including as to attribution (and the confidence in that figure), its timeliness, and its completeness.²⁷⁹ The analysis conducted on the data should preserve such provenance information as is relevant to assessing the confidence that can be placed in any resulting inference drawn or prediction made.

Integrity and security are closely related but separate matters. This discussion focuses on the integrity of data while the data security aspects are considered in 3.5.

3.4.1 Data accuracy

The Data Protection Act 1998 is based on eight principles of ‘good information handling’. The fourth principle addresses data accuracy: ‘Personal data shall be accurate and, where necessary, kept up to date.’²⁸⁰

²⁷⁸ Secretary of State for the Home Department (UK), Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny Cm 9219 (2016) 75-76.
²⁷⁹ There are domain-specific refinements of more general dimensions of information integrity in data systems. For instance the Australian National Audit Office used the term ‘data integrity’ to refer to ‘the consistency, accuracy and reliability of information across [client] records’. See Australian National Audit Office, Audit Report No 28 2008–09: Quality and Integrity of the Department of Veterans’ Affairs Income Support Records (2009) 94.
²⁸⁰ Data Protection Act 1998 (UK), sch 1, pt 1.
This principle finds application in different ways. In respect of police information for example, the Code of Practice on the Management of Police Information,\textsuperscript{281} issued under the Police Act 1996, sets out a number of relevant obligations:

4.3.1 Information should be recorded where it is considered that it is necessary for a police purpose. Chief Officers must establish recording procedures in accordance with guidance issued under this Code.

4.3.2 Where appropriate and in accordance with guidance to be issued under this Code, the source of the information, the nature of the source, any assessment of the reliability of the source, and any necessary restrictions on the use to be made of the information should be recorded to permit later review, reassessment and audit.

4.3.3 Information should be assessed for reliability in accordance with guidance to be issued under this Code.

All police staff members are furthermore required to apply data quality principles to all police information.\textsuperscript{282} It must be:

- **Accurate** – care must be taken when recording information and, where appropriate, the source of the information must also be recorded. If there is any doubt over the authenticity of the information, clarification must be sought from the source. Inaccurate information must be corrected as soon as possible. In ensuring accuracy, it is important not to delete historic information that may be significant (such as details of previous addresses).
- **Adequate** – recorded information must be sufficient for the policing purpose for which it is processed. The nature of the event determines the information that is relevant. All recorded information must be easily understood by others.
- **Relevant** – information recorded must be relevant to the policing purpose. Opinions need to be clearly distinguished from fact.
- **Timely** – information must be promptly recorded into the relevant business area in accordance with agreed timescales.\textsuperscript{283}

Her Majesty’s Inspectorate of Constabulary (HMIC), which reports to the UK Parliament on the efficiency and effectiveness of police forces in England and Wales, has undertaken a program of work over a number of years to test aspects of whether crimes are being recorded by the police when they should be, and categorised correctly.\textsuperscript{284}

### 3.4.2 Considering data integrity in intelligence decisions

Very little information is available in the public domain regarding the safeguarding of data integrity in intelligence decisions by UK agencies.

The reliability of intelligence is, of course, of great relevance and this has been the subject of public inquiries such as the 2004 Butler review of intelligence on weapons of mass destruction.\textsuperscript{285}


\textsuperscript{284} HMIC, Crime Data Integrity <https://www.justiceinspectorates.gov.uk/hmic/our-work/crime-data-integrity/>.  

Reviewing what was known about the weapons of mass destruction in Iraq, the report also considers the processes that are followed to assess the reliability of intelligence:

Intelligence, though it may not differ in type or, often, reliability from other forms of information used by governments, operates in a field of particular difficulty. By definition the data it is trying to provide have been deliberately concealed. Before the actual content of an intelligence report can be considered, the validity of the process which has led to its production must be confirmed. For imagery and signals intelligence this is not usually an issue, although even here the danger of deception must be considered. But for human intelligence the validation process is vital.\(^{286}\)

Reports such as the ISC’s 2014 report on the intelligence relating to the murder of Fusilier Lee Rigby\(^ {287}\) also provide limited perspectives on data and management issues. What is in the public domain, however, tends to indicate a lesser reliance on automated data mining as a detection tool, as the Anderson report noted:

It is sometimes assumed that GCHQ employs automated data mining algorithms to detect target behaviour, as is often proposed in academic literature. That, it would say, is realistic for tasks such as financial fraud detection, but not for intelligence analysis. Much of its work involves analysis based on a fragment of information which forms the crucial lead, or seed, for further work. GCHQ’s tradecraft lies in the application of lead-specific analysis to bring together potentially relevant data from diverse data stores in order to prove or disprove a theory or hypothesis. As illustrated by the case study on GCHQ’s website, significant analysis of data may be required before any actual name can be identified. This tradecraft requires very high volumes of queries to be run against communications data as results are dynamically tested, refined and further refined. GCHQ runs several thousand such communications data queries every day. One of the benefits of this targeted approach to data mining is that individuals who are innocent or peripheral to an investigation are never looked at, minimising the need for intrusion into their communications.\(^ {288}\)

3.4.3 Investigatory Powers Bill: Bulk data, automated analysis and the right to privacy

Clause 225(7) of Investigatory Powers Bill reads:

References in this Act to the examination of material obtained under a warrant are references to the material being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant.

Submissions to the Joint Parliamentary Committee on the draft Investigatory Powers Bill\(^ {289}\) pointed out that the government took the view that automated analysis does not breach privacy. Privacy International, for example said that:

the Government has advanced the argument that an interference with privacy only occurs when data is examined, or ‘read’, by a person as opposed to a machine. We disagree with this position, as ECHR case law makes clear that the interference with privacy occurs at the time of the interception regardless of whether the data is ever ‘read’ by a person.\(^ {290}\)


To the extent that such a view is held, it does not appear to be held consistently in UK legislation. Section 12 of the Data Protection Act 1998 for example allows an individual to file a notice on a data controller to prevent that controller from taking a decision affecting that individual if is informed by automated analysis:

An individual is entitled at any time, by notice in writing to any data controller, to require the data controller to ensure that no decision taken by or on behalf of the data controller which significantly affects that individual is based solely on the processing by automatic means of personal data in respect of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct. 291

A data controller which bases a decision which significantly affects an individual solely on such processing must as soon as reasonably practicable notify the individual that the decision was taken on that basis. The individual may then lodge a request within 21 days for the decision to be reconsidered or for a new decision to be taken on a different basis. 292

This approach and these rights do not extend to the national security and law enforcement realm.

Submissions to the Joint Parliamentary Committee on the draft Investigatory Powers Bill 293 also pointed to the need to mitigate risks that may accompany automated analysis. Paul Bernal, for example, argued that the automated processing required to facilitate such big data analysis comes with additional risks:

Further vulnerabilities arise at the automated analysis stage: decisions are made by the algorithms, particular in regard to filtering based on automated profiling. In the business context, services are tailored to individuals automatically based on this kind of filtering — Google, for example, has been providing automatically and personally tailored search results to all individuals since 2009, without the involvement of humans at any stage. Whether security and intelligence services or law enforcement use this kind of a method is not clear, but it would be rational for them to do so: this does mean, however, that more risks are involved and that more controls and oversight are needed at this level as well as at the point that human examination takes place. 294

The Joint Parliamentary Committee noted the concerns related to automated analysis and made the following recommendation:

We urge the Investigatory Powers Commissioner to scrutinise the automated analysis of bulk datasets conducted by the security and intelligence agencies to ensure that they are conducted appropriately and proportionately and with regard to privacy and data protection requirements. 295

The government responded as follows:

The Government is committed to ensuring that the IPC has the powers, resources and access to specialist knowledge to effectively and visibly oversee the security and intelligence agencies and the use of investigatory powers in the Bill. The Government cannot dictate how the independent IPC must undertake their scrutiny. We expect, and would welcome, though, the IPC scrutinising the automated analysis of bulk datasets. The Bill has been amended to

291 Data Protection Act 1998 (UK) s12(1).
292 Data Protection Act 1998 (UK) s12(2).
make clear that the IPC has access to software and systems. The Government agrees that this would be part of the IPC’s role. 296

While the Investigatory Powers Bill therefore contains various provisions and processes regulating access to datasets for purposes of examination (see 3.1 and 3.2), it does not regulate the automated analysis of the relevant data explicitly. 297 Its examination controls are focused as per clause 225(7) on human inspection of the relevant data.

This is at odds with the approach to automated decisions in the 2016 Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences (also known as the ‘EU-US Umbrella Agreement’). Article 15 requires that decisions producing significant adverse actions concerning the relevant interests of an individual may not be based solely on the automated processing of personal information without human involvement, unless authorised by domestic law, and appropriate safeguards apply, including the possibility to obtain human intervention.

Various provisions deal, however, with controlling the examination of data by humans. Clause 151 for example requires the selection of communications data obtained under a warrant to be carried out only for the purposes specified in the warrant at the time of the selection. The selection of any of the data for examination must furthermore be necessary and proportionate in all the circumstances.

Summary and Implications

The UK has various principles requiring accuracy of data, including keeping data up to date. Control measures in relation to data mining, especially automated data mining, are less comprehensive and clear. There appears to be a view, also embedded in the Investigatory Powers Bill, that protection for data subjects relating to the examination or analysis of their data should apply when their data is read, looked at or listened to by a person but that privacy breaches cannot occur when automated analysis takes place. The Bill therefore does not provide safeguards in relation to automated analysis but does regulate human examination of the data. If the Bill is enacted in its current form, the IPC will, however, have the power to review the automated analysis of acquired data.

3.5 Are data and systems protected?

The fifth line of enquiry considers the rules which protect the security of relevant data and systems. Big Data systems may have a large surface of exposure, impact on more people, and have many facets which all need to be effectively protected, making security issues more challenging and more critical than for systems handling lower volumes of data. As governments increasingly come to rely on the cloud, guidance on cloud security will be relevant for law enforcement and national security uses. The need to discourage the use of more exposed public tools for critical purposes is also enhanced. This is challenging when the system is intended to be accessed and used by a large number of individuals in different agencies and different geographic locations.

Data security is enhanced where agencies maintain proper protocols around the internal reporting of security breaches and concerns. The absence of such measures and support may result in further breaches or unintended release of information.

---

296 Secretary of State for the Home Department (UK), Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny Cm 9219 (2016) 75-76.
297 Appropriate analysis is not a matter addressed by the draft Codes of Practice either. Where relevant, Codes rather focus on limiting access for purposes of examination to preserve privacy. See, e.g., Home Office (UK), Security and Intelligence Agencies’ retention and use of bulk personal Datasets Draft Code of Practice [Spring 2016] 26 [7.5].
3.5.1  Current security requirements under UK Law

The UK’s data security framework rests on a number of key laws and processes.

The UK’s Data Protection Act 1998 is based around principles of ‘good information handling’. The seventh principle addresses data security:

> Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.\(^{298}\)

The principle entails amongst others that several factors need to be assessed to determine appropriate measures:

> Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to -

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected.\(^{299}\)

Non-compliance with the Data Protection Act can lead to the serving of an enforcement notice. Failure to comply with the notice is a criminal offence.

While certain organisations, such as telecommunications service providers are required to notify the Commissioner of Information, and in some cases individuals themselves, of personal data security breaches,\(^{300}\) this requirement does not extend to government agencies. The IC’s 2014/14 annual report noted that of the 1677 reports filed voluntarily, 31 involved police and criminal records and 23 central government.\(^{301}\)

A range of laws criminalise data-related offences. For example:

- The Computer Misuse Act 1990 criminalises unauthorised access to computer material (s 1), unauthorised access with intent to commit or facilitate commission of further offences (s 2); and unauthorised modification of computer material (s 3).
- The Communications Act 2003 also creates relevant offences such as dishonestly obtaining communications services (s 125); possession or supply of apparatus etc. for contravening s 125 of the Communications Act 2003 (s 126) and improper use of public electronic communications network (s 127).\(^{302}\)
- The Wireless Telegraphy Act 2006 criminalises the use of wireless telegraphy apparatus with intent to obtain or disclose information as to the contents of a message without authorization (s 48).\(^{303}\)
- The general fraud offence under the Fraud Act 2006 can be used to prosecute phishing.
- The Regulation of Investigatory Powers Act 2000 criminalises the failure by a decryption key holder with a demand to hand over the key to the police, intelligence services or customs and excise (ss 49-51).\(^{304}\)

\(^{298}\) Data Protection Act 1998 (UK), sch 1, pt 1.

\(^{299}\) Data Protection Act 1998 (UK), sch 1, pt 2.


\(^{302}\) Crown Prosecution Service (UK), Communications Offences <http://www.cps.gov.uk/legal/a_to_c/communications_offences/>.

\(^{303}\) Cl 221 of the IPB envisages amendments to s 48 and related sections of the Wireless Telegraphy Act 2006 (UK).

\(^{304}\) See s 200(4) and sch 10 pt 3 of the IPB for amendments to these provisions.
As far as government data is concerned, data security is also protected by the UK Government Security Classification system that came into effect in 2014. The new system simplifies the previous categories (top secret, secret, confidential, restricted, protect and unclassified) by providing for three classifications (top secret, secret and official). The classification system applies to all information that the UK government collects, stores, processes, generates or that it shares to deliver services and conduct its business.

Each attracts a baseline set of security controls providing appropriate protection against typical threats. Additionally, ICT systems and services may require enhanced controls to manage the associated risks to aggregated data or to manage integrity and availability concerns.

The classifications also impact on choices regarding cloud services. The UK government established a central G-Cloud program with accredited service offerings, subject to appropriate security measures. Organisations are for example advised to manage low risk official information through Assured Public Cloud services that are subject to a suitably scoped ISO27001 certification and other assurance activities as described in the G-Cloud framework documents. Most official information will however be managed through a formally accredited Public Cloud or Private Cloud services, subject to a full government accreditation and be hosted within the UK. In all cases however the agencies concerned should be mindful of the risks involved in outsourcing services and data to the cloud. Off-shoring of information that relates to or supports National Security is, however, prohibited.

The Communications-Electronics Security Group (CESG) – a part of GCHQ – is the National Technical Authority for Information Assurance within the UK. It provides advice on Information Assurance Architecture and cyber security to UK government agencies, critical national infrastructure, the wider public sector and suppliers to UK government.

### 3.5.2 Data Security and National Security Agencies

The RUSI report paid particular attention to the concerns regarding the vulnerability of the increasing volume of data being retained.

The protection of retained data is a major concern for citizens, consumers and businesses. Polling commissioned by the Information Commissioner’s Office (ICO) indicates that 85 per cent of people are concerned about how their personal information is passed or sold to other organisations, and that 77 per cent of people are concerned about organisations not keeping their personal details secure. Just 19 per cent of respondents feel existing laws and organisational practices provide sufficient protection of personal information. A record number of data complaints were made to the ICO in 2013–14, which issued £1.97 million in penalties to companies found in breach of data-protection rules.

A major concern surrounding data retention is that such data may be lost, damaged or stolen by nefarious actors. It is important to highlight that, to date, the UK has not experienced the same scale of private-sector data breaches as can be found in the US. Nevertheless, while UK examples of private-sector data breaches may be considerably

---

309 Cabinet Office, Government Security Classifications (18 October 2013) 33 [52].
310 See discussion in the Australian Report, 3.5.2.
311 Cabinet Office, Government Security Classifications (18 October 2013) 33 [52].
312 Cabinet Office, Government Security Classifications (18 October 2013) [53].
313 See <https://www.cesg.gov.uk/articles/cesg-information-security-arm-gchq>.
smaller in scope, they can still have a significant impact. The 2014 Department of Business, Innovation and Skills’ Information Security Breaches Survey of companies around the UK found that 81 per cent of respondents had detected at least one breach in the previous twelve months. Public attitudes to the security of government-held data have been significantly influenced by high-profile media reports over leaks, losses and thefts. In 2007, for example, HMRC lost the data relating to all families in the UK receiving child benefit payments (approximately 25 million recipients), causing a significant shift in the public’s perception of personal data security.  

The RUSI report also noted several strategies that were implemented to mitigate data security risks, including

- limiting the release of stored data to only relevant information ‘for example, only the relevant sections of a transcript from a telephone interception should be distributed to those with a valid requirement for seeing it’; and
- destruction of stored data by the agencies ‘as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes’, in accordance with RIPA\(^\text{315}\) and the Data Protection Principles.\(^\text{316}\)

This mirrors the information that GCHQ provides on its website regarding its measures to safeguard the data it collects:

> Analysts only ever see the data that matches their properly authorised and legally compliant search terms. Data we collect is held in secure automated systems for a limited period of time and can only be accessed by properly qualified and trained personnel. Analysts must be able to justify their detective work by proving all searches are legal, necessary and proportionate. All justifications are stored, our systems are audited and we have checks in place to review usage.\(^\text{317}\)

RUSI noted, however, that in June 2015, the IPT ruled that, while the interception by GCHQ of the e-mails of two human-rights organisations was legal, it subsequently retained these e-mails for longer than it should have, violating its own internal procedures.\(^\text{318}\)

---


\(^{315}\) See RIPA 2000’s 15(3): ‘The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each copy, made of any of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes.’ See also Anthony May in Interception of Communications Commissioner’s Office, Report of the Interception of Communications Commissioner House of Commons Paper 1113, Session 2014-15 (March 2015) [6.63]: ‘Although my office’s investigation demonstrated that indiscriminate retention for long periods of unselected intercepted material (content) does not occur and the interception agencies delete intercepted material (if it is retained at all) after short periods, and in accordance with section 15(3) of RIPA 2000, I reported that related communications data are in some instances retained for a variety of longer periods and that I had yet to satisfy myself fully that some of the retention periods were justified.’

\(^{316}\) Data Protection Act 1998 (UK), sch 1, pt 1, Principle 5: ‘Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.’

\(^{317}\) GCHQ, FAQs <http://www.gchq.gov.uk/Pages/GCH-Who.aspx>.

\(^{318}\) RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) 22 [1.60]; Liberty v Government Communications Headquarters and others; Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others; American Civil Liberties Union and others v Government Communications Headquarters and others; and other cases [2015] UKIPTrib 13_77-H_2, [2015] All ER (D) 231 (Jun) par 14: ‘In respect of the Third Claimant (The Egyptian Initiative for Personal Rights), the Tribunal has found that email communications of the Third Claimant were lawfully and proportionately intercepted and accessed, pursuant to s.8(4) of RIPA. However the time limit for retention permitted under the internal policies of GCHQ, the intercepting agency, was overlooked in regard to the product of that interception, such that it was retained for materially longer than permitted under those policies. We are satisfied however that the product was not accessed after the expiry of the relevant retention time limit, and the breach can thus be characterised as technical, though (as recognised by the Tribunal in the Belhadj Judgment) requiring a
Encryption is an important element of the data security debate, but one that also provides challenges for law enforcement and national intelligence agencies.

Increased levels of encryption are beneficial in increasing data security for law-abiding users. The challenge for the government, however, is that while it favours encryption as a way of enhancing cyber-security to protect the communications of citizens and companies from criminals, encrypted devices and communications cannot easily be accessed or monitored by law-enforcement and intelligence agencies, even pursuant to a lawful investigation, since the companies themselves will be unable to access the content of the communication.  

3.5.3 Investigatory Powers Bill: Data security and deletion

Various provisions of the Investigatory Powers Bill scheme address data security and deletion obligations.

Submissions to the Joint Parliamentary Committee on the draft Investigatory Powers Bill raised a range of security concerns relating to the retention of large datasets. The concerns focused on potential vulnerability in the hands of providers but obviously also extends to vulnerability of the data when obtained by government. Andrews & Arnold, for example, expressed their concerns as follows:

[R]etention of details of every web site visited reveals much more about a person. It can be used to profile them and identify preferences, political views, sexual orientation, spending habits, and much more. It is also useful to criminals as it would easily confirm the bank used, and the time people leave the house, and so on. This is plainly sensitive personal information, and it is clearly a huge invasion of privacy to collect and retain this information on innocent people. It is also a valuable target for criminals and so a risk for operators to retain this data.

The Home Office responded by assuring the committee that:

The retention systems are built to stringent standards, and those standards are set by the Home Office. Systems do not go live unless they have been independently tested and accredited. We are very confident in the arrangements that we have to maintain security of the data retention systems, and I cannot say more than that. We completely understand the threat, and because of that we put a lot of effort into ensuring that integrity.

The Committee held as follows:

The security of retained data, especially such potentially intrusive data, is of great importance. We have received assurances from the Home Office that it is possible to hold such data securely if high standards are set, observed, and regularly scrutinised but data theft remains an ongoing challenge. We urge the Government to consider the suggestion to work with the Information Commissioner’s Office, the National Technical Assistance Centre and the Communications-Electronics Security Group at GHCQ, which has recognised expertise in this area, to draw up a set of standards for CSPs.
The government responded in part positively to this recommendation:

When setting out the steps that a CSP needs to take to meet its security obligations, the Government already draws upon a set of recognised security standards. Detailed guidance is contained in Chapter 16 of the draft Code of Practice on Communications Data. It is important that CSPs can put in place security safeguards that are appropriate to the nature of the data being retained. The Government will, however, consult the Information Commissioner’s Office, the National Technical Assistance Centre and GCHQ with a view to being able to provide clear and consistent standards for CSPs retaining data under the obligations in the Bill.

As the communications data will be held for purposes that are not related to the CSP’s own business purposes, the Joint Committee agreed that the Government should provide CSPs with the technical and financial support necessary to safeguard the security of the retained data. While the Committee did not agree that the Bill should provide for full cost recovery, it recommended that CSPs should be able to appeal to the Technical Advisory Board on the issue of reasonable costs. The government welcomed the approach and confirmed the longstanding position of reimbursing 100% of the costs associated with data retention.

Clause 213 of the Investigatory Powers Bill 2016 therefore compels the Secretary of State to ensure that arrangements are in force for securing that telecommunications operators and postal operators receive an appropriate contribution in respect of such of their relevant costs as the Secretary considers appropriate. Operators may request the review by the Secretary of contribution levels set out in retention notices. The review process under cl 80 of the Investigatory Powers Bill requires consultation with the Technical Advisory Board and the IPC. The Advisory Board in particular must consider the financial consequences for the provider.

The Bill sets out a range of data security measures, many of which are repeated in relation to data accessed under a specific warrant. For example, in relation to data accessed through lawful interception, clause 46 provides for measures such as:

- Limiting to the minimum necessary for authorised purposes:
  - the number of persons to whom any of the material is disclosed or otherwise made available;
  - the extent to which any of the material is disclosed or otherwise made available;
  - the extent to which any of the material is copied (note however that ‘copy’ has a restricted meaning);
  - the number of copies that are made.

---

324 For similar provisions on the Investigatory Powers Bill relating to other warrants and data, see cl 112 (Safeguards relating to retention and disclosure of material); cl 113 (Safeguards relating to disclosure of material or data overseas); cl 112 (Safeguards relating to retention and disclosure of material); cl 133 (Safeguards relating to disclosure of material overseas); cl 150 (Safeguards relating to the retention and disclosure of data); cl 152 (Offence of making unauthorised disclosure); cl 168 (Safeguards relating to retention and disclosure of material); cl 169 (Safeguards relating to disclosure of material or data overseas); and cl 170 (Safeguards relating to examination of material etc).
325 IPB cl 46(2).
326 IPB cl 46(10): ‘In this section—
‘copy’, in relation to material obtained under a warrant, means any of the following (whether or not in documentary form)—
(a) any copy, extract or summary of the material which identifies the material as having been obtained under the warrant, and
(b) any record which—
(i) refers to any interception or to the obtaining of any material, and
(ii) is a record of the identities of the persons to or by whom the material was sent, or to whom the material relates, and ‘copied’ is to be read accordingly.
- Ensuring that every copy made of any of the material is stored, for so long as it is retained, in a secure manner.\(^327\)
- Ensuring that material obtained under a warrant, if not destroyed earlier, is destroyed as soon as there are no longer any relevant grounds for retaining it.

Under clause 47 the Secretary of State must ensure, in relation to every targeted interception warrant or mutual assistance warrant issued by it, that arrangements are in force for securing that any material obtained under the warrant or copies thereof are handed over to overseas authorities only if the requirements of those requirements of clause 46 are met. Facts such as the existence of an interception warrant as well as any material obtained under it must be kept confidential under clauses 49 and 50 of the *Investigatory Powers Bill*.

The integrity and security of retained by telecommunications operators in terms of the Bill are also protected. Clauses 81 and 82 require operators retaining communications data under the Act to:

- secure that the data is of the same integrity, and subject to at least the same security and protection, as the data on any system from which it is derived,
- secure, by appropriate technical and organisational measures, that the data can be accessed only by specially authorised personnel, and
- protect, by appropriate technical and organisational measures, the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure.

The operator must furthermore destroy the data if the retention of the data ceases to be authorised by the Act, when it is not otherwise authorised by law. That destruction of the data may take place at such monthly or shorter intervals as appear to the operator to be practicable. The operator must furthermore put in place adequate security systems (including technical and organisational measures) governing access to relevant communications data retained by virtue of this Part in order to protect against any unlawful disclosure.

Codes of Practice under the *Investigatory Powers Bill* regime must also regulate security and retention of communications data held by public authorities under Part 3 of the Bill (communications data obtained by authorisation). These must, in particular, include provision about:

- why, how and where the data is held,
- who may access the data on behalf of the authority,
- to whom, and under what conditions, the data may be disclosed,
- the processing of the data for purposes otherwise than in connection with the purposes for which it was obtained or retained,
- the processing of the data together with other data, and
- the processes for determining how long the data should be held and for the destruction of the data.\(^328\)

---

\(^{327}\) *IPB* cl 46(4).

\(^{328}\) *IPB* sch 7 cl 3.
Summary and Implications

The UK has various principles regarding data security but concern was noted that increased data retention under the Investigatory Powers Bill will increase vulnerability of data and data holdings. The government has therefore drafted security standards applicable to communication service providers. It also recognised that providers will retain data for government purposes and therefore government should provide them with the necessary technical support as well as appropriate financial support to safeguard the security of the retained data. ‘Appropriate’ would not seem to amount to full cost recovery. The minister will decide the level of the financial contribution but an operator who is unhappy about that decision may request the minister to review it.

The Investigatory Powers Bill furthermore provides for a range of data security measures including limiting access to, copying and disclosure of data to the minimum necessary for authorised purposes and ensuring that data is destroyed as soon as there are no longer any relevant grounds for retaining it.

3.6 Is accountability maintained?

This section probes aspects of the UK legal and policy framework to determine whether (1) access to data and data analysis and use decisions are tracked and audited for justification, security and intrusiveness, and (2) decisions are subject to appropriate internal governance as well as independent oversight and accountability. As RUSI stated:

Public confidence in the acquisition and retention of data rests on the credibility and practicality of the legal and oversight frameworks that govern it.329

These two aspects are intertwined. They are a useful starting point is to consider the role of the independent accountability structures that are relevant to a Big Data and national security framework. Appropriate governance and accountability measures are vital to ensure the public trust and acceptance of invasive national security measures.

3.6.1 Current oversight and accountability mechanisms

Law enforcement and intelligence surveillance decisions are subject to management oversight, independent oversight and ultimately political and parliamentary oversight.

The Intelligence Services Commissioner for example, described in his 2013 report why, in his opinion, it would require considerable ineptitude or dishonesty of more than one person, including most probably a senior person, to secure an exercise by a Secretary of State of their powers to issue warrants and authorisations, in order to improperly obtain information. His analysis provides an impression of the layers and persons involved in these decisions:

i) [F]or unlawful warrants or authorisations to be issued it would require considerable ineptitude or conspiracy on a massive scale, involving:

- the applicant (in setting out a case for necessity and proportionality)
- the authorising officer (in approving it)
- the lawyers (in signing off or turning a blind eye to illegal activity)
- where ministers are involved the relevant government department warranty unit (in presenting the paperwork for signature)
- the Secretary of State (in signing the warrant)
- the civil servants (who support and advise the Secretary of State)

ii) each agency has an internal legal compliance team. These teams work closely with their legal advisers, senior management and their respective minister (mostly through the

relevant warranty unit) to help ensure that their organisation is operating lawfully and compliantly;

iii) the ethos enshrined within the agencies is one of compliance and it is almost impossible for one person to act without others of some seniority knowing.\textsuperscript{330}

In addition, the system is subject to independent oversight. The Intelligence Services Commissioner noted that if he were to discover such a deliberate decision he would report it to the Prime Minister immediately and notify the Crown Prosecution Service, as those involved would face criminal charges in addition to disciplinary action.\textsuperscript{331}

The UK’s system of oversight for law enforcement and the security and intelligence agencies’ use of investigatory powers is grounded in different Acts, for example RIPA, the \textit{Police Act 1997}, and the \textit{Justice and Security Act 2013 (JSA)}. These Acts provides for oversight by a number of different bodies.\textsuperscript{332}

The Parliamentary oversight function is currently entrusted to the cross-party Intelligence and Security Committee of Parliament\textsuperscript{333} while independent non-Parliamentary oversight is carried out by a number of commissioners:

- The Interception of Communications Commissioner oversees the exercise by public authorities of their interception and communications data powers under RIPA and the powers under section 94 of the \textit{Telecommunications Act} (directions in the interests of national security).\textsuperscript{334}
- The Chief Surveillance Commissioner oversees how law enforcement agencies use covert surveillance powers and covert human intelligence sources under RIPA and the \textit{Police Act 1997}.
- The Intelligence Services Commissioner oversees how the intelligence agencies use the powers available to them under RIPA Part II (covert surveillance and covert human intelligence sources) and the \textit{Intelligence Services Act 1994}.
- The Information Commissioner (IC) has responsibility for promoting and enforcing the \textit{Data Protection Act 1998} and the \textit{Freedom of Information Act 2000}, as well as associated legislation such as the Privacy and Electronic Communications (EC Directive) Regulations 2003.
- The Surveillance Camera Commissioner (SCC), introduced under the \textit{Protection of Freedoms Act 2012}, is primarily focused on raising awareness of, and generating debate on, the use of CCTV in public spaces and other related issues. The Commissioner’s functions include encouraging compliance with the Surveillance Camera Code of Practice.

In addition, the Investigatory Powers Tribunal\textsuperscript{335} investigates and determines complaints of unlawful use of covert techniques by public authorities that infringing the right to privacy and claims against intelligence or law enforcement agency conduct which breaches a wider range of human rights.

While some civil liberties groups are concerned about the current lack of judicial oversight over intelligence and law enforcement agencies, RUSI pointed out that there are significant legal and judicial elements present in the system:

However, there are a number of legal oversight mechanisms currently in place. As noted above, evidence in criminal cases must be admissible in court where it will have to have been first examined by the Crown Prosecution Service before a case is raised. More


\textsuperscript{331} Mark Waller, Intelligence Services (UK), \textit{Report of the Intelligence Services Commissioner for 2013}, (2014).


\textsuperscript{333} \textit{Justice and Security Act 2013 (UK)} ss 1-4.

\textsuperscript{334} \textit{Telecommunications Act 1984 (UK)} s 94. See 3.1.3.

\textsuperscript{335} <http://www.ipt-uk.com/>. 
generally and as discussed below, a number of senior judges hold and have held positions as commissioners, who form a key role in legal oversight. There is also a dedicated tribunal – the IPT – which investigates and determines complaints of unlawful use of covert techniques by public authorities and claims of intelligence or law-enforcement agency conduct breaching human rights. However, it is true to say that the majority of this legal oversight is conducted following the issue of a warrant or other authority; this is true of both the commissioners and the IPT.\textsuperscript{336}

The complexity of the oversight framework was criticised in the Anderson report as well as the reports of the ISC and RUSI. RUSI states:

The roles of the various commissioners are fairly complex and often overlap; even the commissioners themselves require the ‘Surveillance Roadmap’ document to understand what the others do. The document is kept up-to-date as legislation develops, but it describes a regime which the commissioners themselves believe has been somewhat left behind by the pace of technological change, as well as the legal and regulatory developments.\textsuperscript{337}

RUSI also noted a lack of public trust in the oversight framework:

The ISC is the body responsible for holding the SIAs to account. Critics argue that the Committee has ‘consistently, and sometimes very publicly, failed in its duty to challenge these agencies’. These criticisms over its membership, outputs and degree of independent scrutiny have contributed to the deficit in public confidence …\textsuperscript{338}

A second layer of oversight, provided for in legislation, comes in the form of the commissioners – comprising a number of retired senior judges – who, among other functions, retrospectively assess the necessity and proportionality of samples of warrants granting authorisation to intercept citizens’ communications. However, they have also come under criticism, particularly, it is said, because they are ‘only part-time, inspect a small proportion of intercept warrants, have not publicly found a warrant to be disproportionate, have refused to provide adequate statistics and are under-resourced’. Evidence to the ISR Panel suggests that the commissioners and their work is not well known among the general public, and the role of the expert inspectors who support them is equally underappreciated by their critics.\textsuperscript{339}

The Investigatory Powers Bill therefore provides for the creation of a single new independent and more powerful IPC. According to the memorandum to the Bill:

The Commissioner will be properly supported and will have a significantly expanded role in authorising the use of investigatory powers and a wide-ranging and self-determined remit to oversee any aspect of how law enforcement and the security and intelligence agencies use the powers and capabilities available to them.

3.6.2 Current review of decisions regarding access to data, data analysis and use decisions

A range of data-related decisions are currently closely reviewed:

The \textbf{Interception of Communications Commissioner (IOCCO)} for example reviews the interception of communications and the acquisition and disclosure of communications data by the intelligence and security agencies, police and law enforcement, and other public authorities and agencies with


powers to intercept communications. The primary objectives of inspections conducted by IOCCO are to ensure that:

- The systems in place for the interception of communications are sufficient for the purpose of RIPA and that all relevant records have been kept
- All interception has been carried out lawfully and in accordance with RIPA and its Code of Practice
- All errors are reported to the commissioner and that the systems are reviewed and adapted where any weaknesses or faults are exposed.

IOCCO inspectors pay particular attention to questions regarding necessity and proportionality:

During inspections, IOCCO examines warrants submitted by law-enforcement agencies and SIAs and, in particular, the justifications of necessity and proportionality for any interception, as well as whether less intrusive methods were available to achieve the same objective. IOCCO continues to challenge positively the necessity and proportionality justifications put forward by the public authorities to ensure that the significant privacy implications are always at the forefront of their minds when they are working to protect the public in the interests of national security, to save life or to prevent or detect crime.

RUSI also highlighted the questions regarding technical capacity to review coding that filters bulk data:

The ISR Panel were told that the technical work that goes in before the actual interception takes effect is very important, in terms of minimising intrusion and ensuring that large amounts of incidental material are not intercepted. There is a question over whether there is a suitable technological understanding by those overseeing the SIAs to be able to check the coding that filters bulk data and applies the discriminating selectors. So far, IOCCO does not check the code, nor does it currently have the capacity to do so, though it has already begun to discuss with GCHQ what more can be done in terms of testing the code and algorithms, and having greater access to their systems.

The Intelligence Services Commissioner (InSeC) provides independent external oversight of the exercise of intrusive powers, the interference with property, and the investigation of electronic data protected by encryption by the intelligence agencies and parts of the Ministry of Defence. Among others, it is charged with reviewing the exercise by the secretaries of state of their powers to issue warrants and authorisations empowering the intelligence services to carry out their functions, and with the review of decisions of relevant officials within agencies.

The InSeC conducts twice-yearly inspections and ex post facto sampling of authorisations that have been granted by either the secretary of state or the relevant person within the requesting organisation. The InSeC will examine 16–20 per cent of authorisations, checking all the paperwork is in order and confirming that the case of necessity (primary to the case they have to make) and proportionality (concerned with the question of privacy rather than whether adequate resources are available) have been made. Any privacy interference must be justified by the information that is sought.

The Office of Surveillance Commissioners (OSC) performs similar functions to IOCCO and InSeC but in relation to non-intelligence agencies. The OSC has oversight over the use of covert surveillance including the use of covert human intelligence sources by all designated public authorities, except the intelligence agencies overseen by InSeC. The OSC also oversees the exercise of RIPA powers on access to protected data. Its inspections and reviews are not solely paper-based but involves close

interaction with a range of officials. It therefore raised questions of a lack of a level playing field in oversight when oversight over intelligence agencies is compared to oversight over law enforcement agencies.\footnote{RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) 87.}

The OSC does not believe that there is a level playing field across the oversight regime, in terms of the level of scrutiny in place for law enforcement on the one hand and the SIAs on the other. The OSC scrutinises all covert policing departments for up to a week and speaks to a vast array of individuals – from police constables to chief constables, through to heads of agency, and so on. The OSC also scrutinises activity on the front line (including the installation of covert equipment) and explores scenarios with officers of when tactics might be used. This often picks up issues where operatives may not have realised that relevant legislation applies. This is very different to the level of scrutiny by InSeC of the intelligence agencies.

While the OSC has a team approach to its inspections, the InSEC indicated to the ISR that he conducts all inspections personally:

The Intelligence Services Commissioner (currently Sir Mark Waller) conducts all inspections personally, rather than being supported by a team of additional inspectors. Although the InSeC would appreciate greater resourcing, the Commissioner would still rather conduct all inspections personally than be part of an inspection team.\footnote{RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) 86.}

3.6.3 Complaint mechanisms as sources of information and review

The number, nature and content of complaints may provide valuable information to inform the review of current rules and practices relating to data.\footnote{RUSI, A Democratic Licence to Operate: Report of the Independent Surveillance Review (2015) 21 [1.58].}

The protection of retained data is a major concern for citizens, consumers and businesses. Polling commissioned by the Information Commissioner’s Office (ICO) indicates that 85 per cent of people are concerned about how their personal information is passed or sold to other organisations ... A record number of data complaints were made to the ICO in 2013–14, which issued £1.97 million in penalties to companies found in breach of data-protection rules.

**The Investigatory Powers Tribunal**

The Investigatory Powers Tribunal (IPT) functions under RIPA to investigate:

- Interference complaints against a broad range of intelligence, military and law enforcement agencies and other public authorities using covert techniques regulated under RIPA
- Human rights claims relating to the use of covert techniques by intelligence, military and law enforcement agencies and to a wider range of human rights breaches you believe have been committed by the intelligence agencies.\footnote{RIPA 2000 s 65; RUSI Report 92 [4.85].}

The IPT is in essence a special administrative court. It reviews administrative surveillance decisions that may or may not have been taken. It focuses therefore mainly on whether surveillance was appropriately authorised and is conducted in accordance with the applicable rules. It adjudicates surveillance complaints but also has the power and obligation to investigate a complaint lodged with it. This is important as the complainant is generally not in a position to establish the facts. Where a complainant is not under surveillance or correct processes were followed, it makes a determination
of ‘no determination in favour’, as specified by section 68(4)(b) of RIPA. The reason for this rather vague ruling is explained as follows:

It prevents criminals, terrorists or foreign intelligence operatives making serial applications to the Tribunal in order to find out whether they are under investigation and, if they are, how they can avoid detection. Unless the Tribunal has found that there was a breach of the law by the public authority in question, RIPA does not allow the Tribunal to disclose whether someone is of interest to the intelligence or law enforcement agencies or to disclose what evidence it has taken into account in considering the complaint or claim.

The IPT may make any such award of compensation or other order as they think fit, including an interim order and an order:

- quashing or cancelling any warrant or authorisation; and
- requiring the destruction of any records of information which has been obtained in exercise of any power conferred by a warrant or authorisation or is held by any public authority in relation to any person.

The IPT is not obliged to consider or determine any proceedings, complaint or reference if it appears to them that the complaint or reference is frivolous or vexatious. The IPT is also not authorised to hear interference complaints made more than one year after the taking place of the conduct to which it relates, except where the Tribunal are satisfied that it is equitable to hear the complaint.

There is currently no right of appeal on the Tribunal’s decisions to UK courts, other than to the European Court of Human Rights, for matters falling within their jurisdiction. RUSI pointed out that this presents a dilemma for the government as ‘the British intelligence and security services will not submit to foreign judges sitting at the European Court of Human Rights the same material they would submit to the IPT, even if the Court were willing to consider evidence in secret.’ This may weaken the case that the UK presents in the European Court of Human Rights.

The so-called ‘Poole’ ruling (Ms Jenny Paton and others v Poole Borough Council) is one of the IPT’s small number of published rulings. The ruling details the IPT’s finding that it was not necessary or proportionate for Poole Borough Council to undertake surveillance on a family to determine whether they had fraudulent used an in-catchment area address, to obtain a place at a specific school.

A number of recent cases highlighted weaknesses in the processes of the IPT. From the RUSI report:

[4.91] In 2015 in Liberty & Others vs. the Security Service, SIS, GCHQ, the IPT censured GCHQ for failing to provide enough detail on the safeguards on how it shared data with US counterparts until December 2014, although it had previously ruled in December 2014 that the UK intelligence-collection methods did not breach the ECHR. After two additional paragraphs of detail were made public, the agencies were found to no longer have been in contravention of human-rights law.

[4.93] In June 2015, the IPT ruled that communications intercepted by GCHQ relating to the Egyptian Initiative for Personal Rights and the South African non-profit Legal Resources

---

351 RIPA 2000 s 67(6).
352 RIPA 2000 s 67(7).
353 RIPA 2000 s 67(4).
354 RIPA 2000 s 67(5).
355 RIPA 2000 s 67(5).
357 IPT/09/01.
Centre had been retained longer than they should have been. Amnesty International was also one of the claimants in the case, but in the original judgment the IPT made no determination on the organisation’s complaint – implying that either their e-mails and phone calls had not been not [sic] intercepted or that they had been intercepted by legal means. However, the IPT subsequently sent an e-mail to Amnesty correcting the judgment and informing the organisation that it was to Amnesty, not the Egyptian Initiative for Personal Rights, that the ruling applied.\(^{359}\)

The 2015 review reports recognised the IPT as an important mechanisms that requires improvement. Justice summarised the comments as follows in their 2015 report:

> In its recent report, the ISC praised the Tribunal as ‘an important component of the accountability structure’ but nonetheless recommended the introduction of a domestic right of appeal against its decisions. The RUSI panel described the Tribunal as ‘a work in progress’ and made several criticisms of its procedures, including that the Commissioners have no power to refer cases to the Tribunal; secondly, that its rulings were frequently ‘opaque’; that its reliance on complaints brought by the public ‘was not a helpful or just arrangement’; and that its recent confusion between Amnesty International and the Egyptian Center for Personal Rights pointed to the need for ‘clear procedural improvements that will need to be implemented’. It also endorsed the need for a domestic right of appeal.\(^{360}\)

**Whistle-blowing**

The *Public Interest Disclosure Act 1998* provides protection against employer victimisation when an employee blows the whistle in the public interest. While civil servants are in general included in the ambit of this Act, police officers and employees of national intelligence agencies are excluded.\(^{361}\) The *Official Secrets Act 1989* does not provide a public interest disclosure defence for unauthorised disclosures\(^{362}\) and is particularly onerous in relation to officials of intelligence and security services.\(^{363}\) Since 2013, witnesses giving evidence to the ISC do however enjoy protection against incrimination.\(^{364}\)

### 3.6.4 Investigatory Powers Bill: New oversight mechanisms

Improvement of the oversight mechanism was one of the main objectives of the *Investigatory Powers Bill*. The government summarised the proposed scheme as follows:

> The Bill creates a world-leading oversight regime, bringing together three existing commissioners and providing new powers and resources to an independent Investigatory


\(^{360}\) Justice Freedom from Suspicion: Building a Surveillance Framework for a Digital Age (October 2015) par 39 (emphasis in original).

\(^{361}\) *Public Interest Disclosure Act 1998* (UK) ss 10, 11 and 13

\(^{362}\) *R v Shayler* [2002] UKHL 11, [20].

\(^{363}\) Lucinda Maer and Oonagh Gay, ‘Official Secrecy’ (Standard Note No SN/PC/02023, House of Commons Library, United Kingdom, 2008) 7. *R v Shayler* [2002] UKHL 11, [18]: ‘Section 1(1)(a) of the OSA 1989 imposes criminal liability on a member or former member of the security and intelligence services if, without lawful authority (as defined in section 7), he discloses any information or document relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services. The only defence expressly provided is, under subsection (5), that at the time of the disclosure he did not know and had no reasonable cause to believe that the information or documents in question related to security or intelligence. As already demonstrated, a member or former member of the security and intelligence services is treated differently under the Act from other persons, and information and documents relating to security and intelligence are treated differently from information and documents relating to other matters. Importantly, the section does not require the prosecution to prove that any disclosure made by a member or former member of the security and intelligence services was damaging to the interests of that service or the public service generally.’

\(^{364}\) *Justice and Security Act 2013* (UK) cl 7 of sch 1.
Powers Commissioner (IPC). The Commissioner will hold, or have held, high judicial office and will oversee the use of the powers in the Bill by public authorities. The revised Bill strengthens the office of the IPC further. Where the IPC in the course of his or her investigations determines that a person has been the subject of a serious error, the IPC will have the ability to notify the individual concerned.  

Submissions to the Joint Parliamentary Committee on the draft Investigatory Powers Bill raised a range of issues relating to the proposed oversight scheme. The Joint Parliamentary Committee made more than two dozen recommendations for improvements, many of which were adopted by the government.  

Central to both, controls and oversight is the establishment of the office of the IPC and other Judicial Commissioners under cl 194. Each appointee must hold a judicial position of at least senior or a High Court judge. Clause 195 provides that Judicial Commissioners will be appointed for fixed terms of three years and can be re-appointed. As a general rule, they can only be removed from office with agreement of both Houses of Parliament.  

By virtue of cl 196 the IPC and Judicial Commissioners are vested with wide powers to oversee and review the way public authorities intercept communications, acquire or retain communications data and secondary data; or carry out equipment interference, acquire, retain, and use of bulk personal data sets. Under cl 196, the IPC must for example:

- keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to:
  - (a) the interception of communications ...,  
  - (b) the acquisition or retention of communications data,  
  - (c) the acquisition of secondary data or related systems data;  
  - (d) equipment interference.

As part of controls in the form of checks and balances, cl 196(5) provides:

In exercising functions under this Act, a Judicial Commissioner must not act in a way which the Commissioner considers to be contrary to the public interest or prejudicial to—

- (a) national security,  
- (b) the prevention or detection of serious crime, or

---

368 Appointments of Judicial Commissioners will be made by the Prime Minister after consultation with the Lord Chief Justice of England and Wales, the Lord President of Scotland, the Lord Chief Justice of Northern Ireland, the Scottish Ministers, and the First Minister and deputy First Minister in Northern Ireland.
369 Communications data means the details about a communication (the ‘who, when and where’) but not the content of what was said or written.
370 IPB cl 14: ‘(2) In relation to a communication transmitted by means of a postal service, references to obtaining secondary data from the communication are references to obtaining such data in the course of the transmission of the communication. (3) In relation to a communication transmitted by means of a telecommunication system, references to obtaining secondary data from the communication are references to obtaining such data— (a) while the communication is being transmitted, or (b) at any time when the communication is stored in or by the system (whether before or after its transmission)’.  

UK Report draft 24 June 2016 101
The statutory functions of the Commissioner includes undertaking audits, inspections and investigations; to this end, cl 202 mandates disclosure or provision all such documents, information and assistance (include such access to apparatus, systems or other facilities or services) as the Commissioner may require for the purposes of the Commissioner’s functions. Public authorities may ‘report to the Investigatory Powers Commissioner any refusal by a telecommunications operator or postal operator to comply with any requirements imposed by virtue of this Act’, and public authorities, telecommunications operators or postal operators ‘must report to the Investigatory Powers Commissioner any relevant error (within the meaning given by section 198(9)) of which ... [they are] aware’.

The Investigatory Powers Commissioner replaces, among others:

- the Interception of Communications Commissioner, who oversees how public authorities use their interception and communications data powers under the Regulation of Investigatory Powers Act 2000 (UK) and the Telecommunications Act 1984 (UK);
- the Chief Surveillance Commissioner, who oversees how law enforcement agencies use covert surveillance powers and covert human intelligence sources under Regulation of Investigatory Powers Act 2000 (UK), Part II and the Police Act 1997 (UK); and
- the Intelligence Services Commissioner, who oversees how the intelligence agencies use their powers under Regulation of Investigatory Powers Act 2000 (UK) Part II and the Intelligence Services Act 1994 (UK).

The Bill retains the Investigatory Powers Tribunal, but provides it with a range of powers and functions in terms of the Bill and strengthens the right of redress by allowing a domestic right of appeal from the IPT.

**Summary and Implications**

The current UK oversight system regarding access to telecommunication data is generally viewed as complex and public confidence in the effectiveness of the oversight is lacking. The Investigatory Powers Bill therefore aims to create a far better, more consolidated regime. It replaces three existing commissioners and provides new powers and resources to an independent IPC. While the new powers and structures are promising, the effectiveness of the bodies will depend greatly on their staffing and resources.

---

371 See also cl 196(6): ‘A Judicial Commissioner must, in particular, ensure that the Commissioner does not (a) jeopardise the success of an intelligence or security operation or a law enforcement operation, (b) compromise the safety or security of those involved, or (c) unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty’s forces.’ However, by virtue of cl 196(7), ‘Subsections (5) and (6) do not apply in relation to the functions of a Judicial Commissioner of (a) deciding whether to approve the issue, modification or renewal of a warrant or authorisation, (b) deciding what may be done with material when a warrant issued for what was considered to be an urgent need is cancelled, or (c) reviewing any decision of the kind mentioned in paragraph (a) or (b).’

372 The term ‘relevant error’ is defined as error ‘by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner’.

373 IPB cl 206.

374 However, cl 196(4) of the IPB excludes the Investigatory Powers Commissioner oversight from (a) areas that are already subject to oversight by other individuals or bodies; (b) decisions by other judicial authorities; (c) information obtained through a search warrant or production order issued by a judicial authority; and (d) matters which are overseen by the Information Commissioner.

375 IPB cl 208.

376 IPB cl 208.
3.7 Are principles and rules regularly reviewed?

This section highlights mechanisms in the UK legal framework that supports the regular, transparent review of principles and rules to ensure that the system delivers intended results efficiently and reliably, proportional to impacts on civil liberties, other legal rights and individual and commercial interests.

The UK framework provides a range of mechanisms that allow for the review of certain laws, rules and practices. Internal reviews of the effectiveness and efficiency of systems and processes should occur in agencies and also within government as part of the management of the business of government. This inquiry is however concerned with public and independent review mechanisms as these mechanisms impact on the general public trust in the system. In the UK context, public and independent review mechanisms include Parliament, Commissions of Inquiry and independent oversight bodies as well as processes such as regulatory impact assessments and privacy impact assessments.

3.7.1 Review mechanisms

Parliament and government

Parliament provides the forum where new laws concerning data collection, access, disclosure, and use can be debated. Where laws are particularly controversial, the UK parliament sometimes uses mechanisms that require parliamentary re-consideration of statutory provisions, for example the use of renewal by affirmative resolution mechanisms,\(^\text{377}\) and the use of review or sunset clauses. DRIPA 2014 is, for example, subject to a sunset clause in terms of which the Act will cease to have effect from 31st December 2016.\(^\text{378}\) As explained in Chapter 1, this Act was introduced as emergency legislation in response to the 2014 decision of the European Court of Justice of the European Union that the EU Data Retention Directive was invalid. The December 2016 repeal of the provisions of the Act provided impetus for the 2016 adoption of the Investigatory Powers Bill.

Independent Review Mechanisms

The Independent Reviewer of Terrorism Legislation is an important example of independent review mechanisms relevant to this study.

The Reviewer is appointed by the Secretary of State in terms of section 36 of the Terrorism Act 2006 to review the provisions of the Terrorism Act 2000 (a broad instrument addressing among others proscribed organisations, terrorist property, investigations and counter-terrorist powers) and of Part 1 of the Terrorism Act 2006 (terrorism offences and penalties). Reviews are carried out annually and reports are laid before Parliament.\(^\text{379}\) As explained in the Report of the Independent Reviewer on the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006 (2015):

> The function of the Independent Reviewer, as it was explained when reviews were first placed on an annual basis, is to ‘look at the use made of the statutory powers relating to terrorism’, and ‘consider whether, for example, any change in the pattern of their use needed to be drawn to the attention of Parliament’. For more than 35 years, successive

---


\(^{378}\) DRIPA 2014 (UK) s8(3): ‘Sections 1 to 7 (and the provisions inserted into the Regulation of Investigatory Powers Act 2000 by sections 3 to 6) are repealed on 31 December 2016.’

\(^{379}\) Terrorism Act 2006 (UK) s 36.
Independent Reviewers have used their reports to ask whether special powers continue to be necessary for fighting terrorism, and to make recommendations for reform. 380

As part of the political agreement that secured cross-party support for the DRIPA 2014 (see Chapter 1), section 7 was inserted into that Act requiring the Secretary of State to appoint the Reviewer to review the operation and regulation of the relevant investigatory powers, 381 and in particular:

(a) current and future threats to the United Kingdom,
(b) the capabilities needed to combat those threats,
(c) safeguards to protect privacy,
(d) the challenges of changing technologies,
(e) issues relating to transparency and oversight,
(f) the effectiveness of existing legislation (including its proportionality) and the case for new or amending legislation. 382

The report that resulted from this review was one of the trio of 2015 reports on data and investigation (see Chapter 1), and its recommendations informed the Investigatory Powers Bill. 383

The Reviewer played an active role to inform public debate regarding the Bill. 384

The Reviewer considers government policy and statistics and interacts with agencies and community groups. The review process is however not an in-depth inspection function. The Reviewer expresses it as follows, responding to a Supreme Court observation regarding the high level of comfort that could be drawn from the Reviewer’s supervision of port questioning powers: 385

There is a difference between the function of review, as practised by successive Independent Reviewers working alone on a part-time basis, and the inspecting and auditing functions undertaken by other independent figures such as the Chief Inspector of Borders and Immigration or the Interception of Communications Commissioner, in each case with the help of trained inspectors and other staff. While I have devoted considerable time over the past four years to questioning ports officers and ports users, many of my contacts have been at a very senior level; I witness examinations only occasionally; there are still many ports I have never visited; and my efforts could be said to have amounted to ‘continuous supervision’ or to ‘monitoring’ only in a fairly general sense of those words. There are other functions in respect of which the Independent Reviewer is more thinly stretched still; further responsibilities have been or are to be added; and it is desirable to keep some slack in the system for one-off tasks or ‘snapshot’ reports. 386

The Reviewer does not only rely on formal reviews and reports to engage the government and the public. The Reviewer increasingly engages the public actively through posts on its official website,

---


381 DRIPA 2014 (UK) s 7(1).

382 DRIPA 2014 s 7(2).


384 See for example the papers and materials on the Reviewer’s website at <https://terrorismlegislationreviewer.independent.gov.uk/>.

385 David Anderson, Report of the Independent Reviewer on the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006 (2015) 70 [10.16]. The Reviewer was concerned that the Supreme Court placed too high a value on his Review when it stated in DPP v Beghal [2015] UKSC 49, [43] that: ‘the continuous supervision of the Independent Reviewer is of the first importance; it very clearly amounts to an informed, realistic and effective monitoring of the exercise of the powers and it results in highly influential recommendations for both practice and rule change where needed.’

through participation in conferences and other public events and through use of twitter (@terrorwatchdog). According to the Reviewer these additional communication channels enables him to react much faster to developments and often enables him to engage with experts and academics that he would not normally meet in person.  

Commisions of Inquiry
Over the years various ad hoc commission of inquiry have investigated national security legislation and made recommendations regarding law reform and improvement in processes and procedures. Since the introduction of an independent review function, Parliament has not resorted as often to appointing commissions of inquiry, at least in relation to terrorism laws.

Independent Oversight Bodies
The independent oversight bodies discussed in 3.6 also perform important review functions.

3.7.2 Assessment tools
Regulatory impact statements and assessments and privacy impact assessments are important tools that can inform review processes.

The UK government supports the submission of all new policies, programmes and projects, whether revenue, capital or regulatory to comprehensive but proportionate assessment to ensure that the public interest is best promoted. Assessments include appraisals of proposed measures and retrospective evaluation of projects, programs and policies. Assessments may result in a range of outcomes such as business cases; Regulatory Impact Assessment; Health Impact Assessment; Environmental Appraisal; Health and Safety Impact appraisal; Consumer Impact Assessment; Integrated Policy Appraisal; and evaluation and audit reports.

It is UK government policy that government departments and agencies exercising statutory powers and making rules that could affect businesses, charities or the voluntary sector must produce a Regulatory Impact Assessment to assess the costs, benefits and risks of proposed regulation. Assessments should also be produced for proposed European legislation that will have an effect on businesses, the public sector, charities or the voluntary sector in the UK.

UK government departments and agencies as well as the private sector also undertake Privacy Impact Assessments. These generally follow the guidance issued by the ICO. A Privacy Impact Assessment was for example published in November 2015 in relation to the Investigatory Powers

---

Bill. It formed part of a set of impact assessments that covered key aspects of the Bill. The fifteen page Privacy Impact Assessment reviewed the case for the legislation, drawing heavily on the trio of 2015 reports, and briefly reviewed the legislation and proposed safeguards before concluding: ‘It is assessed that implementation of the proposed legislation is capable of being fully compliant with relevant domestic and international law.’

### 3.7.3 Investigatory Powers Bill: Review mechanisms

The Joint Parliamentary Committee on the draft Investigatory Powers Bill recommended that a provision be added to the Bill for post-legislative scrutiny by a committee of the two Houses within six months of the end of the fifth year after the Bill is enacted.

The Government responded by affirming its commitment to post-legislative scrutiny of the Bill:

> Clause 222 requires the Secretary of State to prepare a report on the operation of the Investigatory Powers Act within six years of the Bill being enacted. This is in anticipation of a Select Committee of either House of Parliament (whether acting alone or jointly) undertaking a review of the powers in the Bill within five years and six months of Royal Assent.

In preparing the report clause 222 of the Investigatory Powers Bill 2016 requires the Secretary to take account of any report on the operation of the Act made by a Select Committee of either House of Parliament.

#### Summary and Implications

The UK framework provides a range of mechanisms that allow for or require the review of certain laws, rules and practices. The UK also has a history of usage of sunset clauses for controversial laws. The sunset provisions built into the DRIPA 2014 that provided for its repeal in December 2016, provided urgency and timeframe for the adoption of the Investigatory Powers Bill 2016. A sunset provision was also considered for the Investigatory Powers Bill but in the end the government opted for a post-implementation review five years after the Bill receives Royal Assent. These mechanisms provide valuable opportunities to consider whether the benefits derived from invasive laws are sufficient to retain them.

### 3.8 Is there a sufficient measure of transparency?

Compared to Australia, there seems to be greater awareness in the UK about the importance of transparency and greater sophistication in discussions about how transparency can be accomplished in light of the need for operational secrecy in law enforcement and national security operations.

#### 3.8.1 Transparency as a value throughout the review process

The importance of public transparency was emphasised in all three UK Reports. The Intelligence and Security Committee of Parliament stated:

> ... there is also a legitimate public expectation of openness and transparency in today’s society and, while the Agencies require secrecy in order to conduct much of their work, the Government must make every effort to ensure that as much information as possible is

---


397 Secretary of State for the Home Department (UK), [Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny Cm 9219 (2016) 7].
placed in the public domain. This is essential to improve public understanding and retain confidence in the work of the intelligence and security Agencies. 398

RUSI described transparency as means for enabling the public to engage in informed debate in order to reach agreement on ‘a new, democratic licence to operate’ after the re-invigoration of the debate about privacy and security following the Snowden revelations. 399 Anderson discusses the importance placed on transparency by civil society organisations, describing submissions on the link between transparency and trust (12.6), the importance of clear and transparent authorising statutes in the context of the rule of law (12.9, 12.76), the importance of public debate enabled by clarity and transparency in the operation of powers in practice (12.11, 12.33, 12.35) and the importance of publishing transparency reports with statistics on the operation of the regime in practice (12.16) including oversight mechanisms (12.88). 400 Even the GCHQ has, according to Anderson, ‘expressed a clear intention to be more transparent, wherever possible, about its capabilities and operations’. 401 Anderson himself links transparency with the need to enable public debate (13.2) and to engender trust (13.3).

Transparency to the public cannot, however, be absolute. The dual challenge of enhancing transparency while maintaining operational secrecy was also recognised in all three pre-IPB UK Reports:

The Agencies require access to intrusive capabilities, which they must use in secret. The challenge is how to ensure that the public can be confident that these capabilities are being used appropriately. 402 ... A delicate balance needs to be struck between the legitimate need for public understanding and consent on the one hand, and the risk of inadvertently damaging operational effectiveness on the other. 403

Successive governments have faced a perpetual dilemma: democratic societies demand openness about what is being done in their name but key aspects of the way that police, security and intelligence agencies operate must remain secret in order for their work to be effective. 404

Secrecy is essential to the work of all three Agencies ... If something can be done openly, the Agencies are not needed to do it. This does not mean that they are ungoverned or unaccountable, nor that the need for their activities to be necessary and proportionate is in any way reduced. It does however create a tension with the requirement that the law governing their activities must be accessible and foreseeable. 405

Even producing the reports required navigation of this dual challenge, with the ISC discussing the use of its report to enhance transparency about how data was collected and used by agencies, while also redacting the report to avoid a ‘level of detail that would be damaging to national security’. 406

While there are recognised tensions set out above, none of the reports suggested that one principle should dominate. All recognised that transparency could and should be enhanced. RUSI, for example, recognised that transparency and necessary secrecy are not incompatible, but rather that

cultures of secrecy needed to be confined to operational activities where such secrecy is necessary and in the public interest and not extend to accountability and oversight mechanisms, ethical framework and policy documents, or as means to avoid accountability or hide mistakes.\textsuperscript{407} This is consistent with Anderson’s recommendation that the operation of covert powers remain secret while intrusive capabilities and powers, including their interpretation and justification, be made public.\textsuperscript{408}

Recommendations of the various reports thus emphasised both transparency and secrecy. In all three 2015 reports, the need for transparency and the protected sphere of operational secrecy were not merely abstract, but fed into specific recommendations. For example, the ISC referred to the need for ‘clarity and transparency’ in justifying its recommendation of reform of the \textit{Telecommunications Act 1984}.\textsuperscript{409} Its recommendation that new legislation should clearly list, describe and justify each intrusive capability,\textsuperscript{410} and its recommendation that the Government publish ‘information as to how these arrangements will work (for example, in Codes of Practice).’\textsuperscript{411} Transparency is captured in Anderson’s fourth principle\textsuperscript{412} focussing on clarity in authorising statutes (and underlies a number of his recommendations) as well as more explicitly in recommendations 121-124:

121. It should be recognised that the operation of covert powers is and should remain secret, and that transparency in relation to operational matters is not a realistic goal.

122. Public authorities should be as open as possible (cf ISC Report Recommendation BBB). They should consider how they can better inform Parliament and the public about why they need their powers, how they interpret those powers, the broad ways in which those powers are used and why additional capabilities might be required. They should contribute to any consultations on the new law, so as to ensure that policy-making is informed by the best evidence.

123. The statistics provided by ISIC [Independent Surveillance and Intelligence Commission], a proposed new independent regulator responsible for oversight] should be as informative as possible...

124. Both ISIC and IPT [Investigatory Powers Tribunal], which has jurisdiction to hear complaints in connection with the interception and collection of communications data should be as open as possible in their work, and should seek actively to make the public aware of their role as a check on the powers of public authorities.

Both transparency and secrecy were among RUSI’s ‘Ten Tests for the Intrusion of Privacy’.\textsuperscript{413} Test 6 recognises necessary secrecy which ‘cannot be more than minimally transparent, but ... must be fully democratically accountable’. Test 7 states that ‘secret parts of the state’ must maintain boundaries between what needs to be kept secret and parts of its work that should be openly acknowledged. RUSI’s Test 8 relates specifically to transparency, relating it to the rule of law, and requiring that ‘[a]nything that does not need to be secret should be transparent to the public, not just comprehensible to dedicated specialists but clearly stated in ways that any interested citizen understands.’ This leads to Recommendation 2 that explicitly refers to the need for statutes to be


‘written in plain and accessible language and include details of implementation and technical application of the legislation’.414

Thus all three 2015 reports recognise the need for transparency as a default that should operate absent a need for secrecy in a specific context; all agree that a culture of secrecy should not grow beyond the realm where it is strictly needed for operational effectiveness. One area where all three reports agreed greater transparency could be achieved was through enhanced clarity of the surveillance regime. This may be achieved through a combination of clearly drafted statutory powers, clear boundaries to these powers, clear oversight mechanisms, publication of agency polices and interpretations, as well as public justifications and debates about the statutory regime. The three reports suggest that such measures were an appropriate means of facilitating transparency without crossing over to disclosures of secret operations that may compromise their effectiveness.

3.8.2 Investigatory Powers Bill

Increased transparency was one of the main objectives of the Investigatory Powers Bill. The government explained it as follows:

[T]he Bill makes more explicit the powers available to public authorities to obtain communications or communications data. In doing so, it puts on a clearer statutory footing some of the most sensitive powers and capabilities available to the security and intelligence agencies. Some powers will remain outside of the Bill. For example, in line with the recommendation made by David Anderson QC, the police will retain the ability to use overt search and seizure powers to obtain communications that have been stored on a device or a server, such as emails stored on a web-based server. The Bill also imposes requirements on the Investigatory Powers Commissioner to report to the public and to Parliament precisely how the powers in the Bill have been exercised.415

The increased transparency was generally welcomed by the 2016 reports. A notable exception was the ISC, who expressed disappointment that the draft Bill did not go far enough:

The draft Bill makes some attempt to improve transparency; however, the Committee is disappointed to note that it does not cover all the Agencies’ intrusive capabilities. This failure to address the Committee’s key recommendation means that various powers and authorisations remain scattered throughout different pieces of legislation. As a result, the draft Bill is handicapped from the outset in terms of the extent to which it can provide a clear and comprehensive legal framework to govern the use and oversight of investigatory powers. This is – in our view – a significant missed opportunity.416

The ISC criticised a number of aspects of the draft Bill, including the lack of transparency regarding the concept of ‘operational purpose’:

The draft Bill provides that all Bulk warrants must specify the ‘operational purpose’ for which the material collected is being examined; however, no detail is provided as to what these operational purposes may be. The Committee considers this completely unsatisfactory: it contradicts the primary purpose of the draft Bill, to provide some much needed transparency in this area. The Committee therefore recommends that some detail on the ‘specified operational purposes’ for which material obtained under a Bulk warrant can be examined should be published – only then can Parliament properly evaluate the provisions of the new legislation in this area.

We recognise, however, that it may not be possible to publish full details of the specified operational purposes. In such circumstances, this Committee would expect to be able to

examine the secret material on behalf of Parliament, and to provide assurances or recommendations, as appropriate, to our parliamentary colleagues and to the public. However, the Committee has been told that the list of operational purposes has not yet been finalised by Government, and that it will not be finalised until after the Bill itself has been passed. The Committee is therefore unable to provide any reassurance that these ‘operational purposes’ are appropriate. We fail to see how Parliament is expected to approve any legislation when a key component, on which much of it rests, has not been agreed, let alone scrutinised by an independent body.\textsuperscript{417}

The government responded as follows to this concern:

As the ISC has recognised, it would be contrary to the interests of national security to publish full details of the Operational Purposes. Nevertheless, a list of draft operational purposes has been provided to the ISC in advance of publication of the revised Bill. The list is indicative in that it provides a list of Operational Purposes that might apply in light of the current threat picture. It provides the Committee with a better understanding of the Operational Purposes that the Secretary of State and Judicial Commissioner would be asked to approve when authorising a bulk warrant, to specify the circumstances in which material can be selected for examination.

Further information on Operational Purposes and how this safeguard will work in practice has been provided in the relevant draft Codes of Practice and the operational case for bulk powers, which have been published alongside the revised Bill. The operational case for bulk powers also provides examples of Operational Purposes.\textsuperscript{418}

The Investigatory Powers Bill 2016 increases transparency in one particularly significant respect. Cl 198 requires the IPC to inform a person of any relevant error relating to that person of which the Commissioner is aware if the Commissioner considers that:

(a) the error is a serious error, and

(b) it is in the public interest for the person to be informed of the error.\textsuperscript{419}

For notification purposes a ‘relevant error’ means an error—

(a) by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner, and

(b) of a description identified for this purpose in a code of practice under Schedule 7 of the Act.\textsuperscript{420}

The IPC is required to keep the definition of ‘relevant error’ under review.

For an error to be serious the Commissioner must consider that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person’s rights under the European Convention on Human Rights (within the meaning of the Human Rights Act 1998) is however not sufficient by itself for an error to be a serious error.\textsuperscript{421}

In making a decision whether to notify a person, the IPC must, in particular, consider—

(a) the seriousness of the error and its effect on the person concerned, and

\begin{footnotesize}
\textsuperscript{418} Secretary of State for the Home Department (UK), \textit{Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny} Cm 9219 (2016) 84.
\textsuperscript{419} IPB cl 198(1).
\textsuperscript{420} IPB cl 198(9). The Investigatory Powers Commissioner is required to keep the definition of ‘relevant error’ under review.
\textsuperscript{421} IPB cl 198 (2) and (3).
\end{footnotesize}
(b) the extent to which disclosing the error would be contrary to the public interest or prejudicial to—

(i) national security,
(ii) the prevention or detection of serious crime,
(iii) the economic well-being of the United Kingdom, or
(iv) the continued discharge of the functions of any of the intelligence services. 422

Before coming to a decision Commissioner must ask the public authority which has made the error to make submissions to the Commissioner about the matters concerned. 423

A notification must also inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights, having regard in particular to the extent to which disclosing the details would be contrary to the public interest or prejudicial as set out above. 424

The Commissioner’s annual report must disclose information regarding the number of relevant errors the Commissioner identified; the number that the Commissioner decided was serious errors and the number of persons notified that during that year. 425

Summary and Implications

There is general agreement across the ISC, RUSI and Anderson reports that the current UK system lacks the level of transparency regarding data collection powers required to ensure public trust in the system. The Investigatory Powers Bill aims to increase transparency, especially in relation to the most invasive powers available to public authorities to obtain communications or communications data. In doing so, it puts on a clearer statutory footing some of the most sensitive powers and capabilities available to the security and intelligence agencies. It also provides for the IPC to report to the public how the powers were exercised. The right of the Commissioner to inform a person affected by any relevant serious error, including non-compliance with the new provisions, is another example of an important transparency reform.

422 IPB cl 198(4).
423 IPB cl 198(5).
424 IPB cl 198(6).
425 IPB cl 198(8).
4. CONCLUSION

This study of United Kingdom (UK) was undertaken as a part of a broader comparative study of Big Data and national security (Big Data Technology and National Security: Comparative International Perspectives on Strategy, Policy and Law in Australia, the United Kingdom, the United States, New Zealand and Canada). An overview of the research project, including the research questions, methods and sources of empirical data, and indicators of a legal and policy framework that supports ‘desirable and effective’ Big Data practices can be found in the Methodology Report. Three separate Country Reports—on Australia, Canada and the UK (the current Report)—provide details of the empirical findings and legal analysis in each jurisdiction. Comparative perspectives and recommendations for law reform in Australia are set out in the Comparative Report.

This chapter summarises the key findings and insights from the UK study.

Interviews were conducted between 24 February 2016 and 18 March 2016; the legal analysis presents the law as it stood on 26 May 2016. (While the passage of the IPB through the Commons in early June is noted, there is minimal coverage of changes in the last stages of that passage.)

4.1 Using Big Data for national security: Stakeholders’ perspectives

The empirical research in the UK was designed to provide a comparative dimension to inform our analysis of law and policy for the use of Big Data for national security in Australia. The UK research is based on face-to-face interviews with 14 stakeholders (research participants) who were working in operational agencies (five participants), policy organisations (six participants) or independent bodies (three participants). All were selected because they were able to provide relevant information on the use of data or regulation of data use for law enforcement or security intelligence. Time and resource constraints necessitated a relatively modest sample size. These interview findings are therefore presented with references to the Australian results.

As noted in Chapter 2, the UK and Australian samples were drawn from broadly similar types of organisations (although technical organisations were excluded in the UK) but there were some notable differences in the research participants. The two samples may therefore not be directly comparable.

The interviews explored the following broader themes:

- Current use of data
- Current concerns regarding access to data
- How problems can be overcome
- Big Data: potentials, limits and risks
- Regulation
- Values and Big Data

The goal of this report is to capture understandings, perceptions and views of individual research participants on a range of issues. It is important to emphasise that the empirical findings presented in this report provide a snapshot of the views and perceptions of research participants only. These views and perceptions may or may not be based on a comprehensive or accurate understanding of the issues involved. Given that the sample size is relatively small and not necessarily representative of the population of stakeholders in the UK, the findings are meant to indicate issues and not to be read as a comprehensive coverage of all relevant information. We do not attempt here to evaluate or correct research participants’ views, although we have included cross-references to other sections in the report where appropriate.

4.1.1 Current use of data

General attitudes towards computer technology

Computer technology was viewed as helpful and was regarded as essential to the work of many participants. Digitisation was a particularly important development for intelligence. A significant hindrance in the UK, reflected in comments of the research participants who commented negatively,
focused on the age and nature of computer systems, which were described as inflexible and not
designed for current needs or ‘archaic’.

While all computer systems are built around current needs and use cases, it is important to bear in
mind the need for flexibility in design and in contracts, so that systems can be adapted to meet
future needs over time. Computer systems need to be ‘up to date’ in order to perform what may
come to be regarded as basic functions.

**Types of data used**

Research participants worked with a wide range of data ranging from crime data and intelligence
data (human intelligence, signals intelligence) to social media data and raw data.

As in Australia, research participants in the UK used broad categories to describe the data that they
used, while others focussed on particular databases. One interesting observation, however, was the
fact that, despite the centralisation in the Police National Computer (see 3.1.5), some types of crime
data are held across multiple databases without automated processes to bring datasets together.

**Sharing of data**

As in Australia, data sharing is a highly curated process with different rules for different agencies,
often worked out through negotiated agreements. In many cases, reports are shared rather than
access granted to raw data or databases. Aggregated data may be made available to the public,
sometimes in innovative ways (such as interactive dashboards).

One noteworthy element of UK data sharing arrangements is that the principle of proportionality
seems to have an impact on data sharing arrangements among government departments,
particularly for research and evaluation rather than directly operational concerns. In particular, the
amount of data shared may be minimised, so that the least amount of data is shared to facilitate a
clear purpose. However, much crime data is shared automatically through the use of shared
databases such as the Police National Computer.

**Main purpose of using data**

In the UK, apart from the use of data for crime prevention, criminal investigation and security
intelligence, research participants reported using crime and offender data to conduct research on
offending trends and to evaluate criminal justice programs. It is possible that evidence-based policy
in criminal justice research is more developed in the UK than in Australia, although further
investigation into the Australian situation would be required to draw any conclusions given
differences in sample composition between the two studies and the small sample size.

4.1.2 Current concerns regarding access to data

Three main concerns were raised: legal requirements including privacy issues (real or perceived);
technical issues; and issues relating to ownership of data and trust.

**Legal requirements**: One of the most frequently cited concerns related to real or perceived legal
requirements. General privacy legislation and rules around particular data-sets (such as health data)
posed a barrier to data sharing.

**Technical issues** related to concerns such as the lack of an integrated system, the difficulty (given
the lack of single a national identifier) of cross-linking information across databases, data security
(particularly when exchanging British data internationally) and difficulties of extracting data from
databases that were designed primarily to store data.

---

426 IPB institutionalises this practice through the filter mechanism; see cl 58: Filtering arrangements for
obtaining data; cl 59: Use of filtering arrangements in pursuance of an authorisation, and cl 60: Duties in
connection with operation of filtering arrangements.
Data ownership and trust relate to the reluctance to share agency data with other agencies. This may in part be due to the fear of losing control over information. Lack of awareness outside an agency of data that is held and could be requested was also raised.

Most of the identified barriers to data sharing in the UK were similar to those mentioned in the Australian study. Issues raised in Australia but not the UK include federalism, legal limits on process, different interpretations of legal requirements, compatibility of data formats, handling data volume, reliance on personal relationships, and over-classification. Issues raised in the UK but not Australia include the time taken to negotiate inter-agency agreements, difficulty cross-linking data, technical issues with data extraction and the challenge of knowing what to ask for. While the small sample sizes mean differences should not be over-emphasised, it is possible that these can be explained to some extent by Australia’s federal system and the existence of CrimTrac, as well as the possibility that some legal ambiguities are clarified through inter-agency agreements in the UK.

UK participants provided useful details on rules that apply to international data sharing including the focus on location rather than citizenship for categorising data, the third party rule, the risk of compromising operations, and limitations on data sharing on sensitive topics. These rules are likely also applicable to Australia.

4.1.3 How problems can be overcome

There are some common threads between the suggestions from Australian and British research participants, including a desire to change the political environment (and a recognition this was likely linked to external events). The most useful new insight from the UK study is the suggested formal and informal means through which trust can be built between agencies, including a combination of time, data sharing agreements and joint mission management. The suggestions to move terminology away from ‘data sharing’ and to engage in comparative risk assessment are also worth noting.

4.1.4 Big Data: potentials, limits and risks

What is Big Data?

‘Big Data’ is a term without a single precise meaning; rather it is used to articulate a range of practices. Overall, research participants associated Big Data mainly with concepts of volume and automated analytical capacity. There were, however, a large number of sceptical responses suggesting that the term was either frequently misunderstood or was inherently unclear.

There are no significant differences in the understanding of ‘Big Data’ between UK and Australian research participants. The standard definition, involving the three Vs of volume, velocity and variety also appeared in RUSI’s report (1.36). However, there was much scepticism about the term Big Data among operational and policy participants in the UK; some would prefer the more precise terminologies used in legislation or operations.

Capability of Big Data

There are some interesting observations that can be made about the capabilities attributed to Big Data in the UK. At least in law enforcement, bulk personal datasets (non-specific to intelligence targets, such as telephone records) seem to be used for specific queries only. These are discussed further in sections 3.1.5, 3.2.5, 3.2.8, 3.2.9. Some specific advantages of Big Data— not requiring an advance hypothesis but rather allowing for unforeseen insights, using as evidence, facilitating more data-driven decision-making, identification of targets and identification of patterns and trends – were all raised by UK participants but not in Australia (at least not in those terms). However, scepticism about capabilities was quite strong in the UK, with 4/14 participants making the point that there was a need for caution about expectations.
Use of Big Data
A significantly higher proportion (11/14) of research participants in the UK compared to Australia (14/38) reported that Big Data was being used (sometimes qualified by reference to extent, variation between agencies, or limited knowledge) in their own (operational) work or for law enforcement and/or security intelligence purposes. This is consistent with the view of all research participants who commented that the UK is internationally a leader on data and analytics for law enforcement and national security. Most of the examples of Big Data use were focussed on investigating past events or understanding the present; only three examples concerned predictive analytics. One research participant’s point that ‘curiosity’ was an important factor in the use of Big Data was also of note.

Current use of data analysis tools
As in Australia, operational organisations seem to be using a variety of data analysis and data visualisation tools. Many (3/5) UK operational participants are relying on traditional statistical analysis rather than newer data science techniques.

Barriers/challenges to using Big Data
Research participants in the UK and Australia reported similar types of barriers to the use of Big Data; for example, both groups operated under resource constraints. UK participants were much more likely than Australian ones (9/14 vs 8/37) to focus on technical and resource issues. Although Australian participants nominated legal and privacy barriers most frequently, the proportion of responses was similar to that in the UK sample. Legal issues that were identified in this study reflected the nature of the UK regime, including the requirement for necessity and proportionality (see 3.2). UK participants were more aware than their Australian counterparts that some of the data collected may be incomplete or biased. This concern was not raised by the Australian participants.

Technical and legal barriers are both real. Continuing technical barriers can subvert the intentions of legislators; legal barriers cannot be ignored by technology designers or dismissed as an obstacle to be overcome. Further, those using data science techniques need to bear in mind biases and limitations of the underlying data, which may require an understanding of cultural factors influencing its collection.

Risks of using Big Data
Most of the risks identified in the Australian study were also mentioned in the UK study. The exception was ‘overload’ (which was mentioned by 4 Australian participants), but while that was not recognised as a risk in the UK, constraints on human resources were mentioned as a barrier. In the UK sample, data issues were mentioned more often than legal and privacy issues. Further, some new issues were raised, in particular the risk of a negative impact on freedom of speech, risk of proliferation, the possibility that the outputs would not be useable as evidence in court, and the potential for resources to be misdirected. Some differences in identified risks could be due to the European human rights framework within which the UK operates, and the history of colonialism which gives the UK continuing international influence. The potentially limited use of the outputs of data analytics as evidence in court exists in both countries, but this type of use is not the primary objective in either jurisdiction (see 2.1.5). Similarly, balancing resourcing demands is likely relevant in both jurisdictions. We cannot draw conclusions from risks omitted in UK interviews due to small sample size.

Who is exposed to these risks?
Respondents in the UK and Australia were equally concerned about the broad risk to the community and the risk to disadvantaged groups. They were also concerned about the potential for poor quality decisions if data analytics was done badly and the impact on government of mistakes.
Management of Big Data risks

The main differences in relation to the management of Big Data risks between the Australian and the UK participants were the following: the UK sample had a greater focus on international law and human rights frameworks in the context of regulation, a broader understanding of the different groups that might benefit from education or training, and more emphasis on the idea of public and multi-stakeholder engagement (two way rather than one way communication) combined with greater government transparency. Existing UK initiatives on a data ethics framework, evaluation processes and minimisation of data sharing are also worth noting, as is the suggestion for system warnings when data requests are excessive. The impact of the IPB filtering mechanism on these developments is discussed in sections 3.2.4 and 3.6.2.

4.1.5 Regulation

Laws, regulations, and internal guidelines

Research participants in the UK identified a wide range of legislation and regulatory instruments governing the use of data. Differences between the research/NGO sector and the government sector were limited to the least mentioned categories: European human rights instruments, the Telecommunications Act and national security directions (research/NGO only) and memoranda of understanding, dataset specific legislation, ethical codes and information management requirements (government sector only).

As in Australia, internal guidelines are often a primary reference point within operational agencies. Also similar to Australia, most existing UK laws focus on data collection and access, not data analysis. There were some examples given where the law did potentially restrict data analysis, including the general proportionality requirement, the right to challenge automated decisions and a requirement for ‘fair’ processing. There are further provisions in the IPB. Perhaps most significant is the fact that the requirement for proportionality was mentioned very frequently, cutting across particular identified legislation. The principle would seem to be very familiar within the UK context across a broad range of roles and organisations. This may be due to the fact that the concepts of necessity and proportionality are embedded ‘in the practices and training materials of all public authorities who apply [RIPA]’ (Anderson 5.18). Conversely, the principle of proportionality was only mentioned in two Australian interviews.

Accountability, transparency and oversight mechanisms

As explained in 3.6 the UK oversight regime differs from the Australian regime. In particular, under the current law, there are separate Commissioners and Tribunals that split the role played in Australia by organisations such as IGIS. This regime will be changed under the IPB (see s 3.6). However, as in Australia, the UK relies on both independent/external and internal oversight mechanisms.

---

427 The Data Protection Act 1998 is discussed in more detail in 3.1.2 and 3.4.1.

428 IPB cls 134, 151, 170, 190 and 191.
Appropriateness and effectiveness

Similar to the findings in Australia, UK research participants working in government were generally more positive about laws, regulation and oversight than those in the research/NGO sectors. There is a greater overlap in relevant laws identified between different categories of research participants in the UK compared to Australia. The explanation for differences in views in the UK thus likely rests heavily on differences in values (see 2.6) and challenges of trying to perform particular functions with limited access to data. Opinions about the appropriateness and effectiveness of the Investigatory Powers Bill (earlier version) were mixed. The resulting Bill seems to have resolved some (not all) participants’ concerns about transparency, clarity, simplicity, comprehensiveness and currency of existing laws. However, those concerned that the current legal regime was too permissive retained the same concern about the Bill.

Perceived shortcomings in law and regulation and proposals for reform

Research participants raised a variety of specific and general proposals for reform. Some of these may not be appropriate and others may be based on limited knowledge of the regulatory regime or the participant’s limited viewpoint. It is not our role to make suggestions for law reform in the UK, but the interviews do present a useful picture of some of the controversies in that jurisdiction, at least as they stood in February 2016.

The following suggestions made by UK participants are of interest to the Australian law reform process: (1) suggestions for the conditions under which law reform decisions in this area ought to be made (based on evidence of privacy risks and security benefit, including proper justification for operational cases), subject to transparency issues discussed in 2.6.4; (2) ideas for improving oversight and accountability; (3) the importance of a principles-based regime that is less likely to date quickly; and (4) the importance of clarity and comprehensiveness are worth keeping in mind in developing a better legal framework for Australia.

Regulation by design

Only three UK participants commented on regulation by design; they noted features similar to those discussed in the Australian study including access controls and audit checks. The positive reaction by the NGO cited shows that that particular NGO may have been unaware of the commonness of such measures. Greater publicity of existing measures would have many benefits, including increasing public confidence. There may also be benefits for agencies in sharing ideas for compliance by design with each other. Also of note is the comment by one research participant that ‘[o]fficers won’t trust it if it is wrong once’ and the resulting importance of evaluation prior to deployment.

4.1.6 Values and Big Data

Protections where individual consents to use or sharing of their data (see Methodology Report 5.1)

Research participants in the UK (as those in Australia) mentioned issues around the ‘quality’ of consent, continuing limits on its use (including proper purpose) and security requirements. The issue of expiry or revocation was not raised in the UK study. One interesting issue explored by some research participants is how consent requirements fit with national security and law enforcement exceptions. The idea of ‘societal consent’ could be a useful concept here.
Attitudes to privacy

Research participants in both the UK and Australia had varied views on the importance of privacy, particularly in the context of serious, imminent threats. Similarly, no-one in the UK sample expressed the view that privacy should always be prioritised, although the view was expressed that security threats never justified untargeted intrusions on privacy. While the UK study revealed differences in the relative importance of privacy between different sectors (research/NGO compared to government/independent, the latter being more likely to say privacy should give way), research participants from both ‘sides’ emphasised the importance of following rules relating to oversight, necessity and proportionality. See also 1.1. As observed by one of the participants, there are sometimes ways of improving both privacy and security in which neither is sacrificed.

Privacy versus security: A scenario (see Methodology Report 5.1.2)

As in Australia, most research participants gave the same answers to the scenario whether the context was kidnapping, child sexual assault or terrorism. There were some important differences in the UK responses, including the emphasis on proportionality, the suggestion that data be deleted when it was no longer needed, the suggested need for evidence of reoffending to draw a link with ‘known kidnappers’, and the fact that many potential suspects would already be under surveillance. Also, there was some scepticism about the effectiveness of the hypothesised CCTV face recognition matching tool (in particular by one participant who has developed video analytic tools and one in an operational role).

What transparency is required (see Methodology Report 5.1.8)

In both Australia and the UK, transparency raises questions about competing priorities – operational effectiveness, trade secrets and democratic accountability. Although in the UK some research participants did not believe in transparency about the types of data collected, there was still more concern about disclosure of algorithms than disclosure of data types.

Noteworthy points arising from the UK study include the discussion about oversight and trust and the inevitable reliance on co-operation between oversight and operational agencies. Fuller transparency (for example, direct access to computers) risks undermining that trust and the joint construction of oversight systems. The possibility of post-surveillance disclosure was also a new finding in the UK study.

How views align with others

Although the same differences in opinions existed in the UK as in Australia, the public process through which the law has been changed (including the three reports leading up to the Investigatory Powers Bill) seemed to have narrowed the gap to some extent, or at least clarified the areas of disagreement. However, there remained some distrust between parts of the government and agencies, and the NGO community.

Resolving conflicts in values

As in Australia, differences in values are ultimately settled through democratic elections (Australia report 2.6.6). However, in the UK there were constructive suggestions around further conversations and dialogue, including public workshops, an ethical council or collective problem solving. In some circumstances it may be possible to conduct empirical testing as to matters of fact on which there is disagreement (such as the effectiveness of particular techniques) to the extent this can be done without compromising operational secrecy.

Sources of views

Research participants in the UK formed their views based on similar sources to Australian participants. The recent reports leading up to and following release of the Investigatory Powers Bill were also important in the UK.
4.2 Big Data, law enforcement and national security: The legal environment in the United Kingdom

The study was undertaken during an intensive period of legal and policy development in relation to Big Data, law enforcement and national security in the UK. Public concern about access to data led to the publication of three influential reports in 2015. The reports reviewed a range of matters relating to the current legal framework regulating access to telecommunication data and made recommendations for law reform. In response to the reports and under pressure to meet a sunset clause deadline of December 2016, the government drafted the Investigatory Powers Bill 2016. This Bill adopts terminology and processes to modernise the access and data management regime and improves the quality and consistency of control and oversight measures as well as transparency regarding the exercise of the relevant powers.

The set of indicators developed by the researchers to highlight key aspects of an appropriate framework for fair and effective use of advanced analytics and large data sets for law enforcement and national security purposes, discussed in in Chapter 5 of the Methodology Report, were also applied to analyse the current UK law and relevant measures envisaged in the Investigatory Powers Bill 2016. The analysis was therefore clustered in the following themes:

1. Is access for data mining enabled?
2. Are legal controls comprehensive and proportional?
3. Are legal rules clear, principle-based, consistent and instructive?
4. Is integrity of data and analysis supported?
5. Are data and systems protected?
6. Is accountability maintained?
7. Are principles and rules regularly reviewed?
8. Is there a sufficient measure of transparency?

4.2.1 Is access for data mining enabled?

UK intelligence and law enforcement agencies enjoy extensive access to a wide range of government-held data, including non-clinical health data held by the NHS. Extensive criminal justice and vehicle data is centralised in data bases such as the Police National Computer and supported by a number of advanced analytical capabilities. Automatic Number Plate Recognition (ANPR) technology is for example linked to the UK’s extensive CCTV network and provides automatic number plate recognition while CRIMELINK enables crime and intelligence analysts to identify patterns and links in crimes across the UK. The UK furthermore maintains various capabilities to access and mine social media.

The Investigatory Powers Bill 2016 will not dramatically increase the UK agencies’ access to data but will modernise, clarify and ensure greater consistency relating to, among others, the controls over and processes to access, retain, examine, exchange and delete private communications data. A new requirement to keep internet connection records will add to the data that can be accessed under the Bill. The Bill does not regulate automatic data mining, only human examination of data.

4.2.2 Are legal controls comprehensive and proportional?

The current legal regime regarding access to and retention, examination, exchange and deletion of private communications data is out-dated and lacking in public trust.

Under the current regime, metadata can be accessed on the strength of an authorisation issued by senior officials within the requesting agency while access to content data requires a warrant issued by a minister. Authorisation and warrants may only be issued if tests of lawfulness, necessity and proportionality are met, and processes may be inspected independent oversight bodies to ensure that appropriate tests were applied.

The Investigatory Powers Bill 2016 will improve control measures by increasing the clarity and consistency of control measures. In particular, it deals with rules for data including large data-sets as
templates to be adhered to by all agencies based not on the nature of the agency that has generated, gathered and manages them, but in accordance with the characteristics of the data-set in question (bulk, interference with equipment, etc.), and the nature of usage (access, sharing, retention, etc.)

It retains the important tests of lawfulness, necessity and proportionality but introduces judicial review for the exercise of the most intrusive powers by means of a so-called double-lock system. This system is embedded in warranty procedures that have been streamlined and standardised. The Bill furthermore enhances oversight and transparency to improve public trust in the operation of the system.

4.2.3 Are legal rules clear, principle-based, consistent and instructive?

The current regime enabling access to telecommunications data and its retention, analysis, sharing and destruction is unclear and inconsistent. In addition the terminology and processes have not kept up with technological developments. The lack of clarity provides room for confusion and undermines public trust in the system. The Investigatory Powers Bill 2016 was therefore drafted with the objective to clarify the law.

The Bill employs improved terminology reflecting current technological concepts. It standardises authorisation and warranty processes and improves overall consistency in relation to control and oversight measures. Different groups hold different views about the level of clarity of some of the terms and measures, but, given the complexity of the subject matter and the range of issues to be addressed, perfect clarity and simplicity are due to remain evasive.

4.2.4 Is integrity of data and analysis supported?

The UK has various principles requiring accuracy of data, including keeping data up to date.

Control measures in relation to data mining, especially automated data mining, are less comprehensive and clear. There appears to be a view, also embedded in the Investigatory Powers Bill 2016, that protection for data subjects relating to the examination or analysis of their data should apply when their data is read, looked at or listened to by a person but that privacy breaches cannot occur when automated analysis takes place. The Bill therefore does not provide safeguards in relation to automated analysis but does regulate human examination of the data. If the Bill is enacted in its current form the IPC will, however, have the power to review the automated analysis of acquired data.

4.2.5 Are data and systems protected?

The UK has various principles regarding data security but concern was noted that increased data retention under the Investigatory Powers Bill 2016 will increase vulnerability of data and data holdings. The government has therefore drafted security standards applicable to communication service providers. It also recognised that providers will retain data for government purposes and therefore government should provide them with the necessary technical support as well as appropriate financial support to safeguard the security of the retained data. ‘Appropriate’ would not seem to amount to full cost recovery. The minister will decide the level of the financial contribution but an operator who is unhappy about that decision may request the minister to review it.

4.2.6 Is accountability maintained?

The current UK oversight system regarding access to telecommunication data is generally viewed as complex and public confidence in the effectiveness of the oversight is lacking. The Investigatory Powers Bill 2016 therefore aims to create a far better, more consolidated regime. It replaces three existing commissioners and provides new powers and resources to an independent IPC. While the
new powers and structures are promising, the effectiveness of the bodies will depend greatly on their staffing and resources.

4.2.7 Are principles and rules regularly reviewed?
The UK framework provides a range of mechanism that allow for or require the review of certain laws, rules and practices. The UK also has a history of usage of sunset clauses for controversial laws. The sunset provisions built into the DRIPA 2014 that provided for its repeal in December 2016, provided urgency and timeframe for the adoption of the Investigatory Powers Bill 2016. A sunset provision was also considered for the Investigatory Powers Bill but in the end the government opted for a post-implementation review five years after the Bill receives Royal Assent. These mechanisms provide valuable opportunities to consider whether the benefits derived from invasive laws are sufficient to retain them.

4.2.8 Is there a sufficient measure of transparency?
There is general agreement across the three 2015 reports (ISC, RUSI, Anderson) that the current UK system lacks the level of transparency regarding data collection powers, required to ensure public trust in the system. The Investigatory Powers Bill 2016 aims to increase transparency, especially in relation to the most invasive powers available to public authorities to obtain communications or communications data. In doing so, it puts on a clearer statutory footing some of the most sensitive powers and capabilities available to the security and intelligence agencies. It also provides for the Investigatory Powers Commissioner to report to the public how the powers were exercised. The right of the Commissioner to inform a person affected by any relevant serious error, including non-compliance with the new provisions, is another example of an important transparency reform.