A Democratic Licence to Operate

Report of the Independent Surveillance Review

RUSI
www.rusi.org

Royal United Services Institute
for Defence and Security Studies

A Democratic Licence to Operate

Report of the Independent Surveillance Review

Royal United Services Institute
for Defence and Security Studies

Over 180 years of independent defence and security thinking

The Royal United Services Institute is the UK's leading independent think-tank on international defence and security. Its mission is to be an analytical, research-led global forum for informing, influencing and enhancing public debate on a safer and more stable world.

Since its foundation in 1831, RUSI has relied on its members to support its activities, sustaining its political independence for over 180 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

Published in 2015 by the Royal United Services Institute for Defence and Security Studies.

Whitehall Report 2-15, July 2015. ISSN 1750-9432

Printed in the UK by Stephen Austin and Sons, Ltd.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Acronyms and Abbreviations

ANPR	Automatic number-plate recognition
ASH	All Source Hub
CEG	Communications Exploitation Group
CHIS	Covert human-intelligence source
CSP	Communications service provider
CTIRU	Counter Terrorism Internet Referral Unit
CTSA 2015	Counter-Terrorism and Security Act 2015
DPA 1998	Data Protection Act 1998
DRIPA 2014	Data Retention and Investigatory Powers Act 2014
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ECtHR	European Court of Human Rights
EU	European Union
FBI	Federal Bureau of Investigation
FCO	Foreign and Commonwealth Office
GCHQ	Government Communications Headquarters
GDS	Government Digital Service
HMRC	Her Majesty's Revenue and Customs
HRA 1998	Human Rights Act 1998
ICO	Information Commissioner's Office
ICT	Information and communications technology
InSeC	Intelligence Services Commissioner
IOCCO	Interception of Communications Commissioner's Office
IoT	Internet of Things
IP	Internet Protocol
IPT	Investigatory Powers Tribunal
ISA 1994	Intelligence Services Act 1994
ISC	Intelligence and Security Committee of Parliament
ISIL	Islamic State of Iraq and the Levant
ISR	Independent Surveillance Review
JIC	Joint Intelligence Committee
MI5	Security Service
MLAT	Mutual legal assistance treaty
NCA	National Crime Agency
NGO	Non-governmental organisation
NISO	National Intelligence and Surveillance Office
NSA	National Security Agency
NSC	National Security Council
OECD	Organisation for Economic Co-operation and Development
ONS	Office for National Statistics
OSC	Office of Surveillance Commissioners

PICs	Priorities for Intelligence Collection
RIPA 2000	Regulation of Investigatory Powers Act 2000
RUSI	Royal United Services Institute
SCC	Surveillance Camera Commissioner
SIAs	Security and intelligence agencies (MI5, SIS and GCHQ)
SIS	Secret Intelligence Service (also known as MI6)
SMS	Short Message Service
SSA 1989	Security Service Act 1989
T&Cs	Terms and conditions
Tor	The Onion Router
UK	United Kingdom
UN	United Nations
URL	Uniform Resource Locator
US	United States of America

Preface

BRITAIN IS AN open, democratic and increasingly digital society. Technological innovation and the growth in global communication networks have enabled commerce, trade and the transfer of knowledge. British citizens, companies and the government have embraced the benefits of these ever-expanding national and international networks.

The availability of digital technology is having a profound effect on society. Computers guide our everyday activities and regulate our communications. Big data is reshaping the way we live, work and think. Digital information is helping us to identify social trends, tackle crime and prevent disease.

More information and data is being shared: between citizens themselves; between citizens and government; consumers and companies; and exchanged by the public and private sectors. Often this information is shared across national borders. Protecting privacy and ensuring data security is necessary but is thus becoming more difficult as information volumes increase and are moved and stored around the world.

The strain of technological evolution on society is particularly acute in the realms of crime, national security and public safety. Technological developments have enhanced the capacity of governments, companies and citizens to know more about individuals and to undertake surveillance, interception and data collection. The Internet has become the front line in contemporary debates about privacy and security.

Privacy is an essential prerequisite to the exercise of individual freedom, and its erosion weakens the constitutional foundations on which democracy and good governance have traditionally been based in this country.

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. These agencies are dependent on the public's consent, and in an open society there is therefore an important understanding between citizens and the state that the agencies must operate within a strict legal framework, that their intrusions into private life must be necessary and proportionate, and that they must be overseen and scrutinised by independent bodies.

In Britain how these principles apply in practice in the digital age has been the subject of considerable controversy, with recent reviews concluding that the state of the law has not matched the pace of technological change.

Antiquated laws will neither keep the public safe nor ensure individual privacy. This is particularly true as the Internet and communications technologies have an impact on our national security, public safety and individual privacy. The UK is vulnerable to states and non-state actors looking to use cyberspace to steal, compromise or destroy critical data.

While the benefits and risks of a technology-dependent, data-based society are increasingly apparent, the trade-offs that may be required to protect the UK's open, liberal and democratic society are only now being fully explored and understood. For some, the free and open nature of the Internet represents these values and there should be no compromise. However, governments cannot ignore threats to national security and public safety that have emerged from the growth of, and our increasing reliance on, the Internet and communications technology, and must remain able to uphold the law and protect the public.

The citizen's right to privacy online as offline – and what constitutes a 'justifiable' level of intrusion by the state – has become a central topic of debate. As traditional notions of national security and public safety compete with the realities of a digital society, it is necessary to periodically renew the licence of the police, security and intelligence agencies to operate. This report aims to enable the public at large to engage in a more informed way in the debate, so that a broad consensus can be achieved and a new, democratic licence to operate can be agreed.

Panel of the Independent Surveillance Review
July 2015

Executive Summary

THE BRITISH PUBLIC are entitled to some answers following the disclosures made by Edward Snowden in 2013. He alleged, among other things, that the UK and US governments were conducting mass surveillance programmes. The Independent Surveillance Review (ISR) was undertaken at the request of the then deputy prime minister partly in response to this very serious allegation.

The ISR Panel's terms of reference were to look at the legality of UK surveillance programmes and the effectiveness of the regimes that govern them, and to suggest reforms we felt might be necessary that would both protect individual privacy as well as the necessary capabilities of the police and security and intelligence agencies (SIAs).

This Review has tried to interpret its terms of reference from the perspective of the British citizen so that it can add the greatest value to other reports that have examined similar issues from Parliamentary and legal perspectives. The ISR Panel think there are inadequacies in present arrangements and offer three groups of recommendations to try to address them. The Panel are not concerned with 'surveillance' in all its manifestations – which cover many standard aspects of policing and intelligence work – but primarily with the interception and use of private communications and related data.

The British population has been greatly affected by the rapid evolution in information and communications technology. In this digital society, we all leave extensive traces of our behaviour and interactions in the course of our normal, everyday lives. We have unprecedented opportunities to express ourselves, to connect and share knowledge, to be prosperous and inventive.

At the same time, the digital society also presents new challenges, making citizens potential targets for fraudsters, criminals and possibly terrorists. The task for the police and SIAs has become more demanding as they try to stay abreast of rapid technological innovation and deal with threats that emanate from across the globe. It is important to ensure that the powers granted to these agencies to protect the public are explicit, comprehensible, and are seen to be both lawful and consistent with democratic values.

Despite the disclosures made by Edward Snowden, we have seen no evidence that the British government knowingly acts illegally in intercepting private communications, or that the ability to collect data in bulk is used by the government to provide it with a perpetual window into the private lives of British citizens.

On the other hand, we have seen evidence that the present legal framework authorising the interception of communications is unclear, has not kept pace with developments in

communications technology, and does not serve either the government or members of the public satisfactorily. A new, comprehensive and clearer legal framework is required.

The SIAs have covert and intrusive powers that enable them to delve into people's personal lives, and considerable technical capabilities to do this, including the ability to intercept substantial volumes of data from across the Internet and then filter and analyse what they have collected. The ISR Panel consider that our privacy rights as individuals are engaged whenever these agencies embark upon such intelligence activity, including when the public's data is accessed, collected, filtered and eventually examined by an intelligence analyst. At each stage, such activities must be demonstrably lawful, necessary and proportionate. Such requirements are essential if there is to be public confidence in the use of these powerful capabilities.

Public confidence in the work of the police and SIAs is generally high. But such confidence is less evident in the way the public thinks its communications and other data are used by government. The ISR Panel conclude that there are inadequacies both in law and oversight that have helped to create a credibility gap that has undermined the public's confidence.

To address this credibility gap we believe that recommendations in three key areas should be considered by the government.

The first is in the process of authorisation for any intrusion into a citizen's private life. Warrants are an established and important legal mechanism authorising the use of the state's most intrusive powers. They are crucial in being able to monitor, record and audit the use of such powers. The current system of warrantry (the issuing of warrants) is complex, incomplete and lacks legal clarity, particularly in light of outdated assumptions such as the distinction between domestic and international communications. The ISR Panel believe the system requires a radical overhaul which must include an enhanced role for the judiciary.

The second is in the oversight regime that ensures the police and SIAs are held to account. It is neither possible nor desirable for those parts of the state that must operate in secret to be fully transparent, but effective oversight is therefore all the more essential. The current oversight regime operates in a series of layers, from ministerial oversight, parliamentary oversight, to the work of a number of judicial commissioners and the Investigatory Powers Tribunal (IPT). This system has grown in ad hoc ways and the public have limited knowledge and understanding of how it works. In the past few years a number of improvements have been made to the oversight regime, but further reform is required. Reorganisation and better resourcing of the existing setup could create a more streamlined, robust and systematic oversight regime that would be genuinely visible to the public and have a positive effect on the police and SIAs.

The third is in the articulation of enduring principles that the ISR Panel believe must be set before Parliament and the public as new legislation is considered. In the past, the government's licence to operate secretly was implicit, not least because the SIAs were not officially acknowledged. The situation today is radically different and the public have greater expectations of openness and transparency in government. It is not sufficient for the government to assume it has public consent for the secret parts of its work just because it had it in the past. To that end the ISR Panel offer ten tests that any new legislation or regulation must be seen to pass before Parliament and the public can have confidence in it, and which also guarantee the ability of the police and SIAs to continue to go about their work. We regard these tests as the essence of a democratic licence to operate now and for the future.

Ten Tests for the Intrusion of Privacy

1. **Rule of law**: All intrusion into privacy must be in accordance with law through processes that can be meaningfully assessed against clear and open legislation, and only for purposes laid down by law.
2. **Necessity**: All intrusion must be justified as necessary in relation to explicit tasks and missions assigned to government agencies in accordance with their duly democratic processes, and there should be no other practicable means of achieving the objective.
3. **Proportionality**: Intrusion must be judged as proportionate to the advantages gained, not just in cost or resource terms but also through a judgement that the degree of intrusion is matched by the seriousness of the harm to be prevented.
4. **Restraint**: It should never become routine for the state to intrude into the lives of its citizens. It must be reluctant to do so, restrained in the powers it chooses to use, and properly authorised when it deems it necessary to intrude.
5. **Effective oversight**: An effective regime must be in place. Effectiveness should be judged by the capabilities of the regime to supervise and investigate governmental intrusion, the power it has to bring officials and ministers to account, and the transparency it embodies so the public can be confident it is working properly. There should also be means independently to investigate complaints.
6. **Recognition of necessary secrecy**: The 'secret parts of the state' must be acknowledged as necessary to the functioning and protection of the open society. It cannot be more than minimally transparent, but it must be fully democratically accountable.
7. **Minimal secrecy**: The 'secret parts of the state' must draw and observe clear boundaries between that which must remain secret (such as intelligence sources or the identity of their employees) and all other aspects of their work which should be openly acknowledged. Necessary secrecy, however, must not be a justification for a wider culture of secrecy on security and intelligence matters.
8. **Transparency**: How the law applies to the citizen must be evident if the rule of law is to be upheld. Anything 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.

9. **Legislative clarity**: Relevant legislation is not likely to be simple but it must be clearly explained in Codes of Practice that have Parliamentary approval, are kept up-to-date and are accessible to citizens, the private sector, foreign governments and practitioners alike.
10. **Multilateral collaboration**: Government policy on intrusion should be capable of being harmonised with that of like-minded open and democratic governments.

Recommendations

Legislation

Recommendation 1: We support the view – as described in both the Intelligence and Security Committee of Parliament (ISC) and Anderson reports – that the current surveillance powers are needed but that they require a new legislative framework and oversight regime. We do not believe that the ISC's recommendation of consolidating all current laws relating to the intelligence agencies in a single legal framework is required to achieve substantial reform, nor do we think there should be separate legislation for the police and for the security and intelligence agencies. We agree with David Anderson's suggestion that RIPA 2000 Part I, DRIPA 2014 and Part 3 of the CTSA 2015 should be replaced by a comprehensive new law.

Recommendation 2: The new legislation should be clearly articulated while also recognising the complexity of the issues. Codes of Practice, published in statute, should be written in plain and accessible language and include details of implementation and technical application of the legislation.

Recommendation 3: Following evidence received by the ISR Panel and further discussion with civil-liberties groups and communications service providers (CSPs), we recommend that definitions of content data and of communications data[1] should be reviewed as part of the drafting of new legislation. They should be clearly delineated in law.

Police, Law Enforcement and Local Authorities

Recommendation 4: While the number of public authorities with the power to obtain communications data has recently been reduced, we believe (i) that there should be a periodic review of which public bodies have the authorisation to use intrusive powers (such as directed surveillance and interception of communications) and (ii) that all relevant applications from authorised public bodies to obtain communications data must be made via the National Anti-Fraud Network as the national single point of contact in the future.

Recommendation 5: A national approach to policing in the digital era is necessary and long overdue. The police require a unified national digital policing strategy and the resources to deliver the capability to ensure digital investigations and intelligence capability. This will require a co-ordinated national effort bringing the relevant bodies together, and a review of core training in digital investigations and intelligence skills for all officers.

1. Communications data is the 'who, where, when and how' of a communication, but not its content.

Advisory Council for Digital Technology and Engineering

Recommendation 6: A Technical Advisory Board was established under RIPA 2000 which brought together industry experts in a personal capacity. Since its inception, the Board has not met regularly and is seen as ineffectual. The government should replace the Board with an Advisory Council for Digital Technology and Engineering. The Advisory Council would be a statutory and non-departmental public body established under new legislation. Terms of reference for a new Advisory Council should be drawn up so as to keep under review the domestic and international situation with respect to the evolution of the Internet, digital technology and infrastructure, as well as:

- Provide advice to relevant ministers, departments and agencies on technical measures
- Promote co-operation between the public and private sectors
- Manage complaints from CSPs on notices and measures they consider unreasonable
- Advance public education
- Support research on technology and engineering.

Recommendation 7: The Advisory Council should be a resource for a new National Intelligence and Surveillance Office (see Recommendation 17) and the ISC.

Bulk Collection of Data

Recommendation 8: The capability of the security and intelligence agencies to collect and analyse intercepted material in bulk should be maintained with stronger safeguards as set out in the Anderson Report. In particular, warrants for bulk interception should include much more detail than is the case currently and be the subject of a judicial authorisation process, save for when there is an urgent requirement (see Recommendation 10, point 2).

The Warrantry Regime

Recommendation 9: We agree with both the ISC and Anderson reports that there should be different types of warrant for the interception and acquisition of communications and related data, and have drawn on both sets of recommendations. We recommend three types of warrant for the interception of communications and an authorisation for communications data:

1. For the interception of communications in the course of transmission we suggest two different types of warrant:
    a. A *specific interception warrant* which should be limited to a single person, premises or operation
    b. A *bulk interception warrant* which would allow content data *and* related communications data to be obtained.

2. For the acquisition of communications data in bulk, a *bulk communications data warrant* which would be limited to the acquisition of communications data
3. For the acquisition of communications data otherwise than in bulk, an *authorisation* by the relevant public authority. Communications data should only be acquired after the authorisation is granted by a designated person.

Judicial and Ministerial Authorisation of Warrants

Recommendation 10: We recommend that the government adopts a composite approach to the authorisation of warrants, dependent on the purpose for which the warrant is sought and subsequent degree of ministerial input required. Our approach does not discriminate between whether it is law enforcement or an intelligence agency submitting the warrant.

1. Where a warrant (see points 1a, 1b and 2 in Recommendation 9) is sought for a purpose relating to the detection or prevention of serious and organised crime, the warrant should always be authorised by a judicial commissioner. Most police and other law-enforcement warrants would fall into this category. A copy of each warrant should be provided to the home secretary (so that the home secretary and officials can periodically examine trends in serious and organised crime, for example)
2. Where a warrant (see points 1a, 1b and 2 in Recommendation 9) is sought for purposes relating to national security (including counter-terrorism, support to military operations, diplomacy and foreign policy) and economic well-being, the warrant should be authorised by the secretary of state subject to judicial review by a judicial commissioner. The review should take place before implementation of the warrant. If there is a case of urgency the secretary of state should be able to direct that a warrant comes into force immediately, and the judicial commissioner should be notified straight away and the judicial review conducted within fourteen days.

The judicial commissioners in charge of the authorisation of warrants should not be part of a new National Intelligence and Surveillance Office nor should they be based in a government department, but alternative office facilities should be sought so that the commissioners are accessible but remain independent. To ensure no loss of operational efficiency, appropriately qualified judges would have to be available at all times throughout the year.

Investigatory Powers Tribunal

Recommendation 11: The Investigatory Powers Tribunal (IPT) should be as open as possible and proactively find ways that make its business less opaque to the public.

Recommendation 12: The IPT should hold open public hearings, except where the Tribunal is satisfied that private or closed proceedings are necessary in the interests of justice or other identifiable public interest.

Recommendation 13: The IPT should have the ability to test secret evidence put before it by the SIAs. While internal procedures are a matter for the Tribunal to decide, we suggest that this could be achieved through the appointment of a special counsel.

Recommendation 14: We agree with both the ISC and Anderson reports that the domestic right of appeal is important and should be considered in future legislation.

Recommendation 15: Appointment to the IPT should be limited to a term of four years, renewable once for a further four years.

Recommendation 16: The judicial commissioners should have a statutory right to refer cases to the IPT where they find a material error or arguable illegality or disproportionate conduct.

A National Intelligence and Surveillance Office

Recommendation 17: The Intelligence Services Commissioner, Interception of Communications Commissioner's Office, and the Office of Surveillance Commissioners should be replaced by a new single independent organisation: a National Intelligence and Surveillance Office (NISO). This organisation should be placed on a statutory footing and its independence guaranteed by statute.

Recommendation 18: A NISO should have an office based outside of the Whitehall departments, have a public profile and be led by a senior public official. The new organisation should be staffed by appropriate persons with technical, legal, investigative and other relevant expertise (for instance in privacy and civil liberties). The new organisation would have four main areas of responsibility:

- Inspection and audit
- Intelligence oversight
- Legal advice
- Public engagement.

Recommendation 19: A NISO should provide support and assistance to the Investigatory Powers Tribunal and the judicial commissioners.

Mutual Legal Assistance Treaties

Recommendation 20: Urgent improvements are necessary in order to expedite the mutual legal assistance treaty (MLAT) process and, in particular, to the UK–US process

in managing data requests. We support the practical reforms suggested by Sir Nigel Sheinwald to the existing MLAT between the UK and the US, to include the greater standardisation of processes, training and improved guidance. The scope for a new and wider international framework between like-minded democratic countries should also be seriously investigated 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.

Introduction

0.1 On 4 March 2014, the then deputy prime minister, the Rt Hon Nick Clegg MP, announced an independent review of surveillance practices in the UK. The Independent Surveillance Review (ISR) would be conducted by the Royal United Services Institute (RUSI) under the chairmanship of its director general and publish its report after the general election of May 2015.

0.2 The terms of reference for the ISR were as follows:

- Advise on the legality, effectiveness and privacy implications of the UK surveillance programmes, particularly as revealed by the 'Edward Snowden case'
- Examine 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
- Make an assessment of how law-enforcement and intelligence capabilities can be maintained in the face of technological change, while respecting principles of proportionality, necessity and privacy.

0.3 A panel for the Review was identified. The twelve members agreed to serve in a private capacity, and were carefully selected to represent the major stakeholders on surveillance issues: government, industry, civil society and Parliament. The panel for the Independent Surveillance Review comprised:

- Professor Heather Brooke
- Lesley Cowley OBE
- Lord Evans of Weardale KCB DL
- Professor John Grieve CBE QPM
- Professor Dame Wendy Hall DBE FRS FREng
- Professor Lord Hennessy of Nympsfield FBA
- Baroness Lane Fox of Soho CBE
- Professor Sir David Omand GCB
- Baroness O'Neill of Bengarve CH CBE FBA FRS
- The Rt Hon the Lord Rooker
- Sir John Scarlett KCMG OBE
- Professor Ian Walden.

0.4 The ISR Panel was chaired by Professor Michael Clarke, director general of RUSI. The biographies of the Panel can be found in Annex A. RUSI provided a secretariat to assist in scheduling meetings, undertaking research and drafting the report.

0.5 The ISR Panel met with a broad range of organisations and individuals and held seventeen evidence sessions. It received a number of submissions. A list of evidence can be found in Annex B. A bibliography can be found at the end of the report.

0.6 The ISR Panel visited the three British security and intelligence agencies (SIAs – comprising MI5, SIS and GCHQ), the National Crime Agency (NCA) and Metropolitan Police. We are grateful to the Foreign and Commonwealth Office (FCO) and Home Office for their co-operation and assistance.

0.7 The ISR was initiated following the unlawful disclosure of classified information in June 2013 by Edward Snowden, a US employee of contractors for the National Security Agency (NSA). From documents provided by Snowden, it was reported that the NSA was collecting the telephone records of US customers of Verizon, an American broadband and telecommunications company. The order, granted by the Foreign Intelligence Surveillance Court, required Verizon on an 'on-going, daily basis' to give the NSA information on all telephone calls in its systems, both within the US and between the US and other countries.[1] Approximately 58,000 documents also related to the UK Government Communications Headquarters (GCHQ) which, it was also reported, tapped the fibre-optic cables that carry vast amounts of global communications. The government has, with only a few exceptions, maintained its traditional line of neither confirming nor denying matters relating to national security.

0.8 This report, A Democratic Licence to Operate, is one of several publications that have followed these disclosures (we provide a brief overview of the relevant findings from these reports in Chapter V). In October 2013, the Intelligence and Security Committee of Parliament (ISC) announced that it would be broadening its inquiry into the laws which govern the ability of intelligence agencies to intercept private communications, to include work on the appropriate balance between individual rights to privacy and collective rights to security. The ISC's report was published in March 2015.

0.9 Following the announcement of the creation of the ISR led by RUSI, the government asked David Anderson QC, the independent reviewer of terrorism legislation, to review the legislation governing the use of communications data and interception, with particular regard to the following issues:

- Current and future threats, capability requirements and the challenges of current and future technologies
- The safeguards to protect privacy
- The implications for the legal framework of the changing global nature of technology
- The case for amending or replacing the legislation
- The statistical and transparency requirements that should apply

1. Glenn Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily', *Guardian*, 6 June 2013.

- The effectiveness of current statutory oversight arrangements.

David Anderson's report was published in June 2015.

0.10 The ISR Panel have also taken into consideration a number of other reports, including the report by the Joint Committee of Parliament on the Draft Communications Data Bill and the annual reports of the Intelligence Services Commissioner, Interception of Communications Commissioner and Surveillance Commissioners, all of whom are senior retired judges.

0.11 Finally, the ISR Panel have considered the outputs of non-governmental initiatives such as Don't Spy on Us, a coalition of privacy and civil-liberties groups including Big Brother Watch, the Open Rights Group and Privacy International; Reform Government Surveillance, an alliance of some of the world's most influential Internet companies including Google, Facebook, Microsoft and Apple; and the Global Commission on Internet Governance, chaired by the Swedish politician and diplomat Carl Bildt, and featuring two of the ISR Panel as members. The Global Commission was established to articulate and advance a strategic vision for the future of Internet governance and has put forward its own proposals for a new social compact.

0.12 The ISR Panel's wide-ranging evidence sessions have helped to make clear the complex ecosystem that citizens and consumers understand as 'the Internet', but which is made up of multiple networks and communications technologies that rest on a sophisticated infrastructure spanning the globe.

0.13 This report takes into account certain issues that the ISR Panel thought were important to consider, but which were beyond the remit of other reviews and inquiries. These included the distinct challenges faced by law-enforcement agencies (including police forces, the NCA, HM Revenue and Customs, among others) in comparison to the SIAs, as well as the role of the private sector in data collection and retention.

0.14 Chapter I describes the rapid pace of change in communications technology, the evolution of the Internet infrastructure that supports it, and the opportunities and challenges that this presents for society. It also outlines the volume and value of data being created by citizens, companies and government in the modern digital society.

0.15 Chapter II looks at the concepts and qualified rights of privacy and security, as well as known public attitudes to data collection, surveillance and privacy.

0.16 Chapter III is concerned with the challenges of the digital age, the Snowden disclosures and what they revealed about the operation of the UK's security and intelligence apparatus. It explores the scope of work the police and SIAs are required to undertake, and which provides the legal justification for their intrusion into citizens' lives.

0.17 Chapter IV outlines the frameworks of legality and accountability within which government surveillance operates. These are key aspects of any new, or renewed, licence to operate for the police and SIAs.

0.18 Chapter V reflects on the work of the ISC and the government-commissioned report of David Anderson, both of which explore different aspects of privacy and surveillance in the UK and make a number of recommendations for change. As these recommendations are considered, we suggest the key questions which the public should ask and which the current Parliament should debate. We offer our support for certain themes inherent in existing recommendations, before outlining a number of our own.

I. The Digital Society in an Information Age

1.1 The Internet underpins our everyday lives, from the critical national infrastructure we rely on for water and electricity, to modern commerce and public communications. The development of networked computer technologies has transformed the way in which individuals communicate, consume, work and engage across the spheres of social, economic, political and cultural life.[1] The Internet is simultaneously a worldwide broadcasting capability, a mechanism for information dissemination and a medium for collaboration and interaction between individuals and organisations, without regard for traditional national boundaries.[2]

1.2 While the introduction of the Internet has had a major influence on modern society, its development has, in turn, been affected by its rapid take-up and the growth in the number of users globally. The pace of technological change and consumer-adoption rates associated with information and communications technology (ICT) are unprecedented. The proportion of UK households with Internet soared from 13 per cent in 1999 to 46 per cent in 2002, 57 per cent in 2006, and 84 per cent (22 million households) in 2014.[3]

1.3 The British public have become accustomed to living in a digitally networked society. According to data from the Office for National Statistics (ONS), in 2014 over three-quarters of the British adult population (38 million adults) accessed the Internet every day.[4] The convergence of communications technology and software with portable handsets has led to a rapid uptake of mobile phones, portable computers and handheld devices, and has enabled access to the Internet on the go. Access to the Internet using a mobile phone more than doubled in the UK between 2010 and 2014, from 24 per cent to 58 per cent.[5]

1.4 Calls and SMS (text) messaging are no longer the primary communication means attached to a mobile phone. In light of developments in mobile technology, many of the most popular social-media platforms rely on the data capabilities of smartphones. In many cases, these platforms exist *only* on smartphones, as in the case of Snapchat, Instagram

1. Yvonne Jewkes and Majid Yar (eds), *Handbook of Internet Crime* (Milton: Willan, 2009), p. 1.
2. Barry M Leiner et al., 'Brief History of the Internet', Internet Society, <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet>.
3. Office for National Statistics, 'Internet Access – Households and Individuals 2014', Statistical Bulletin, August 2014.
4. *Ibid.*
5. *Ibid.*

and Tinder, for example.[6] According to the ONS, over half (54 per cent) of all UK adults participated in social networking in 2014, including 91 per cent of adults aged 16 to 24.[7]

1.5 Our method of producing, consuming and trading goods and services has also adapted to the digital age. The digital technology sector grew over seven times faster than the economy as a whole between 2008 and 2013.[8] Amazon has been the dominant online retailer of recent years, having seen an 838 per cent increase in sales since its inception in 1997.[9] Online-only entertainment services are growing, and Netflix and YouTube now account for more than half of all traffic over the Internet by volume. Industries ranging from railways to retail all depend on high-performance ICT systems to maintain essential business communications with both customers and suppliers. In the financial sector, business worth hundreds of billions of dollars is transacted daily via public and private global data networks. In the public sector, vital institutions rely on ICT to deliver critical health, education and social services.[10] Modern trade and commerce is significantly facilitated by the Internet, not only in terms of communication (especially via e-mail) and logistics, but also processing and exchanging financial and business information. The ability to collect and use consumer data has enabled the private sector to target its communications and advertising at particular groups of consumers and to provide more personalised services.

1.6 The Internet is a key medium for democracy and protest and is changing the relationship between governments and citizens. Research conducted by the Hansard Society found that the Internet makes it 'easier to take part in democracy', and suggested that citizens 'want to communicate and engage, to track and contribute to the democratic debate'.[11] At the same time David Kaye, the UN special rapporteur on freedom of opinion and expression, warns that contemporary digital technologies provide governments – as well as corporations, criminals and pranksters – with an 'unprecedented capacity to interfere with the rights to freedom of opinion and expression'.[12]

1.7 The Internet is changing how governments operate too. A Digital Efficiency Report published in 2012 explained why 'going digital' was important to the British economy. The report estimated that between £1.7 and £1.8 billion could be saved and 'digital services can harness the power and convenience of the web to make these interactions quicker,

6. *The Economist*, 'The Truly Personal Computer', 28 February 2015.
7. Office for National Statistics, 'Internet Access – Households and Individuals 2014'.
8. Department for Culture, Media and Sport and HM Treasury, 'The Digital Communications Infrastructure Strategy', Policy Paper, 18 March 2015.
9. Amazon, 'Amazon.com: 2014 Annual Report', 2015.
10. Paul Cornish, Rex Hughes and David Livingstone, 'Cyberspace and the National Security of the United Kingdom' (London: Royal Institute of International Affairs, 2009), p. 1.
11. Andy Williamson, 'Digital Citizens and Democratic Participation: An Analysis of How Citizens Participate Online and Connect with MPs and Parliament', Hansard Society, 2010.
12. David Kaye, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', UN Human Rights Council, A/HRC/29/32, 22 May 2015, p. 3.

simpler and more secure'.[13] The Government Digital Service platform for services, the gov.uk site, received 2 billion visits in its first two years.[14] The Verify scheme, a product of the Government Digital Service, is also now in place. The service allows people to verify their identity online by allowing users to register securely using one login that connects and securely stores their personal data.[15]

1.8 While the trend suggests that more services will be put online, evidence points to the vulnerability of governments that are heavily dependent on Internet-based services. For example, Estonia has developed an extensive Internet infrastructure and has moved to make almost all government services online – including online voting, medical prescriptions and parking tickets. Yet in May 2007, Estonia was the target of a sustained DDoS attack, which brought down government websites, media and financial institutions for three weeks. In addition to land, sea, air and space, cyberspace is now being considered as a possible 'fifth domain' of modern warfare, and Internet-enabled actions are increasingly recognised as a possible form of hostile state action.[16]

1.9 Citizens, companies and governments have eagerly taken advantage of the immense opportunities the Internet has created but remain 'uncertain about its longer term effects and implications'.[17] The Internet was never designed to be secure, and the way that it has evolved creates systemic vulnerabilities that can be exploited by criminals and those who wish to do harm.

1.10 The pace of change is also a challenge for those who are responsible for policy, legislation and regulation. Many of the individuals and organisations that provided the ISR Panel with evidence highlighted the lack of technical expertise in senior positions in government. The journalist and author Misha Glenny makes a useful analogy in his book *DarkMarket*: as is the case with motor cars, we now find ourselves in a situation where only a handful of people have a significant understanding of the Internet and how it functions, compared to the billions of people who use it regularly. It is important for both individuals to have this understanding (to protect personal data and reduce vulnerabilities) as well as government officials (to implement appropriate laws and regulations).

Digital Britain

1.11 The British population remain largely unaware of the complex global infrastructure that supports the Internet. Not only is this infrastructure largely invisible, but it is notoriously

13. Cabinet Office and Government Digital Service, 'Digital Efficiency Report', Research and Analysis, 2012.
14. Government Digital Service and Cabinet Office, 'About the Government Digital Service', Blog, <https://gds.blog.gov.uk/about/>.
15. Cabinet Office and Government Digital Service, 'Introducing GOV.UK Verify', Guidance, 17 June 2015.
16. NATO, 'Wales Summit Declaration', Press Release (2014) 120, 5 September 2014.
17. Tim Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', *Contemporary Security Policy* (Vol. 33, No. 1, April 2012), pp. 148–70.

complex and difficult to understand, particularly as it continues to evolve. There are a number of layers of infrastructure required in order to send information from one computer to another over a network. The ISR Panel were interested in three layers in particular: the device layer, network layer and physical layer. It is within these layers that citizens, companies, police and SIAs primarily come into conflict with one another.

1.12 The **device layer** consists of computers, smartphones and the software applications that they house – we can now access the Internet via laptops, tablets, smartphones and wearable devices from a variety of different manufacturers and suppliers.

1.13 The **network layer** is a catch-all for protocols that allow network functionality. The Internet is a vast network of networks – networks which operate using free and openly available protocols, allowing anyone to create a network and connect it to all other networks on the Internet. A system known as packet switching is used to break down and group data into suitably sized chunks – packets – that can be sent via multiple routes across the network. Devices called routers calculate the most efficient route to send these data packets (packets from the same connection will not necessarily be sent via the same route), and the data is reconstituted at the other end by the recipient device. All information sent over the Internet uses the Internet Protocol (IP), a set of global standard operating procedures. When a person connects their device to the Internet, their communications service provider (CSP) normally assigns them an IP address. This IP address works in much the same way as a postal address or telephone number, allowing the device to communicate with other devices across the Internet. Sometimes the IP address used in communicating is the same as that permanently assigned to a device (a static address) and does not change. Given the enormous expansion in recent years in the number of Internet-enabled devices and the limited number of IP addresses currently available, however, devices are often assigned temporary, dynamic IP addresses for the period of the communication, and which change for each session.[18]

1.14 CSPs such as BT, Vodafone or Virgin Media provide access to internet and telephony services through their network infrastructure, but the same term can also be used of application providers, such as Facebook or Twitter. There are several hundred CSPs and internet service providers (ISPs) in the UK providing access services. BT, TalkTalk, Sky, Vodafone, O2, Everything Everywhere, Virgin Media and Three are among the largest.[19]

1.15 Within much of the existing legislation governing telecommunications services in the UK, the definition of a CSP is purposely broad to ensure that the legislation remains technology-

18. The move towards the latest version of the Internet Protocol, IPv6, sees the adoption of 128-bit IP addresses, as opposed to the 32-bit addresses of IPv4. This allows for an exponentially greater number of addresses to be generated, potentially reducing the need for dynamic assignment.
19. Intelligence and Security Committee of Parliament (ISC), *Access to Communications Data by the Intelligence and Security Agencies* (London: The Stationery Office, 2013).

neutral.[20] As part of their routine business processes, CSPs retain information on their customers and the use of their services, such as recording the telephone numbers called by a customer to allow itemised billing. Both CSPs and ISPs also hold names, addresses and bank details in order to bill customers, and they monitor and retain information about traffic passing across their networks to help improve the services they offer.[21]

1.16 Regarding **the physical layer**, in the past twenty-five years telecommunications services have expanded rapidly to support cellular and satellite phones and wireless connection to the Internet, in addition to the physical cables and exchanges that make up the telecommunications infrastructure. This vast global telecommunications network forms a vital part of the UK's critical national infrastructure and is the regular target of attack by both state and non-state actors.[22] The largest telephone network remains that run by BT which reaches everywhere in the UK (except Hull), while smaller telecommunications companies have constructed their own smaller 'figure of eight' networks connecting London, Bristol, Birmingham, Manchester and Leeds – paralleling the early deployments of both canals in the eighteenth century and railways in the nineteenth.[23] These telecommunications networks include major lines designed to handle many signals simultaneously, connecting major switching centres or nodes. Traditionally, these lines were made up of copper cables, though there has been increased investment over the past ten years in national fibre-optic networks, which are able to send much larger amounts of data over longer distances. Satellite links provide a relatively small part of the international bandwidth; the preferred choice for CSPs to transfer information internationally has been to invest in submarine communications cables, as shown in Figure 1 – most of which today are fibre-optic cables.

20. The definition of 'telecommunications service' is described in Section 2 of the Regulation of Investigatory Powers Act 2000. The Communications Act 2003 also adopts a broad, technology-neutral definition (in Section 32), but which is narrower than that used in the Regulation of Investigatory Powers Act 2000.
21. ISC, *Access to Communications Data by the Intelligence and Security Agencies*.
22. ISR Panel visit to GCHQ, December 2014.
23. Electronic Communications Resilience and Response Group, 'Telecommunications Networks – a Vital Part of the Critical National Infrastructure', Version 1.1, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62279/telecommunications-sector-intro.pdf>; *The Economist*, 'The Truly Personal Computer'.

Figure 1: Global Submarine Cable Map.

Source: <http://www.submarinecablemap.com/>

1.17 The use of submarine cables is an evolution of the first cables that carried telegraph messages at seven words a minute in the late nineteenth century. The first international fibre-optic cable connected the UK and Belgium in 1986. Each cable may consist of multiple 'bearers'[24] and there are approximately 100,000 such bearers joining up the Internet.[25] Today, a single cable can carry millions of telephone calls, together with huge amounts of Internet data, such as video.[26] Given the UK's location between the US and Europe, an estimated 10 to 25 per cent of the world's Internet traffic transits the UK via submarine cables.[27]

The World Wide Web

1.18 The three layers described above are part of the architecture of the Internet. For most people, their use of the Internet is via the World Wide Web (henceforth, the Web). While many people use the words Internet and Web interchangeably, they are different. The

24. Each fibre optic cable may carry several 'bearers' which can carry up to 10 gigabits of data per second.
25. ISC, *Privacy and Security: A Modern and Transparent Legal Framework* (London: The Stationery Office, 2015), p. 26.
26. International Cable Protection Committee, 'About Submarine Telecommunications Cables', 2011, <https://www.iscpc.org/publications/>.
27. David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* [Anderson Report] (London: The Stationery Office, 2015), p. 51.

Internet is a global system of interconnected computer networks. In contrast, the Web is one of the services available over these networks.[28]

1.19 The decentralised and, it was perceived, egalitarian nature of the early Web was eroded by commercialisation, which began in earnest in the 1990s. As a result, 'The belief that "peripheral voices" could move centre stage in the digital era – central to a naive mid 1990s view of the Internet – became increasingly implausible'.[29] As commercialisation increased and large Internet firms began to emerge, companies sought to track user preferences and habits online in order to improve the efficiency of the system. One means of achieving this was the development of 'cookies' – text files that were placed on an Internet user's hard drive by their web browser in order to log information about their behaviour. In May 2011 a 'cookie law' was adopted by all EU member states that requires websites to gain consent from visitors to store or receive any information on a computer or web-connected device.[30]

1.20 The initial purpose of these kinds of user-tracking technologies was for companies to better understand their users and improve services, as well as to prevent crimes such as infringement of intellectual property rights. It was not long before crimes committed on the Internet began to attract the attention of governments and law-enforcement agencies, which could see the movement of traditional, 'offline' crimes into the online sphere. An increasing proportion of crimes are perpetrated with an online component – whether traditional crimes now conducted on a much bigger scale, such as fraud and child sexual abuse, or those exclusive to an Internet environment, such as computer viruses and other forms of malicious software (malware).

The Dark Web

1.21 When accessing information on the Web, most people use search engines. However, a traditional search engine can only find information that is open and public to all, and that has been indexed by the automatic programmes used by search-engine companies. Known as the 'surface web', this represents a small percentage of the total content of the Web. The vast majority of content on the Web is found on the 'deep web' – unindexed by search engines, comprising protected websites such as the intranets of companies and governments, and e-mail, document- and photo-storage sites.

---

28. World Wide Web Consortium (W3C), 'Description of W3C Technology Stack Illustration', <http://www.w3.org/Consortium/techstack-desc.html>.
29. Yvonne Jewkes and Majid Yar, *Handbook of Internet Crime*, p. 26.
30. The 'cookie law' was adopted in 2002, requiring notification to users. See European Communities, 'Directive 2002/58/EC of the European Parliament and of the Council', *Official Journal of the European Communities* (L201, 2002), Art. 5(3), p. 44. The addition of a consent obligation was 'adopted' through an amendment in 2009, which came into force in May 2011. See European Union, 'Directive 2009/136/EC of the European Parliament and of the Council', *Official Journal of the European Union* (L337, 2009).

1.22 A small portion of the deep web, known as the 'dark web', is only accessible via special browser software such as The Onion Router (Tor). Like the original Internet, Tor is the result of research conducted by the US government with the original purpose of protecting intelligence communications online. It was promulgated by the State Department to help dissidents avoid the surveillance of authoritarian governments around the world. The software maintains the privacy of both the source and the destination of data and the people who access it. It does this in part by routing connections through servers around the world, making the IP address of the user much harder, if not virtually impossible, to trace.

1.23 The existence of Tor and other similar technologies has thereby allowed the dark web to develop and users to maintain anonymity online. This has positive and negative implications. On the one hand, it allows individuals to circumvent censorship and access websites blocked by authoritarian regimes, as well as share confidential and sensitive information more securely and anonymously. This anonymity, however, also offers advantages to those undertaking criminal activities online.

1.24 In particular, Tor allows people access to so-called 'hidden' services. The most infamous of these sites was Silk Road, a black-market bazaar, where illegal drugs and other illicit goods and services were regularly bought and sold by the site's users. Other dark-web sites specialise in selling malware to hackers and enabling child pornography to be exchanged. During the visit of the ISR Panel to the Metropolitan Police, senior officers expressed concern not only at the use of such dark-web sites, but also about increased levels of online encryption, particularly as cyber-crime is now a volume crime.[31]

Encryption

1.25 Encryption is the process of converting information into an unreadable form, so that only someone with the decryption key can read it. Encryption has been fundamental to the development of major Internet services. Numerous online activities, from sending e-mails to shopping and banking transactions, depend on encryption to ensure security and maintain consumer confidence. For example, web browsers are able to encrypt credit-card details when a user is making a purchase using a protocol for secure communications called HTTPS; when this is enabled, a small padlock appears in the corner of the browser and the website address starts with https://.

31. ISR visit to the Metropolitan Police, April 2015. The Association of Chief Police Officers (ACPO) defines volume crime as: any crime which, through its sheer volume, has a significant impact on the community and the ability of the local police to tackle it. Volume crime often includes priority crimes such as street robbery, burglary and vehicle-related criminality, but can also apply to criminal damage or assaults. See National Policing Improvement Agency, 'Practice Advice on the Management of Priority and Volume Crime (The Volume Crime Management Model)', 2nd edition, 2009.

1.26 Asymmetric (or public-key) cryptography involves encrypting data with a pair of keys. Each user has a public key, which can be made openly available, and a private key that is kept secret. Once information has been encrypted by another party using the intended recipient's public key, nobody but the holder of the counterpart, private key can decrypt it (in reverse, if the private key is used for encryption, anyone with the public key can decrypt it).[32] The first widely available public-key encryption software was Pretty Good Privacy (PGP), released in the 1990s as a response to the US government's attempt to control encryption via a proposal by the NSA, known as 'Clipper Chip'.[33] Typically, the server a user connects to provides the encryption for an Internet session, in order to provide security during the transmission process. Increasingly, however, companies have begun to offer end-to-end encryption for all interactions over their network, providing security in such a way that only the end recipients, not the company server relaying the data, can decrypt the message.[34] According to evidence given to the ISR Panel by providers, data privacy has become an important issue for customers; offering services using sophisticated levels of encryption can provide a commercial advantage over competitors.

1.27 The trend towards more common use of encryption pre-dates the Snowden disclosures,[35] and has been affected by other factors, including incidents such as the high-profile hacks on celebrity Apple iCloud accounts in 2014, among many others. The subsequent privacy-enhancing changes introduced by Apple include encrypting data by default on iPhone devices – a move also made by Google in respect of Android devices. The encryption of material on the iPhone is now user-controlled, meaning even Apple is now unable to unlock securely configured iOS 8 devices.[36]

1.28 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. The encryption challenge was outlined by James B Comey, the director of the FBI, in a speech to the Brookings Institution in 2014 where he described two overlapping challenges:

32. Parliamentary Office of Science and Technology, 'Data Encryption', Postnote, No. 270, 2006.
33. Anderson Report, p. 60.
34. *Ibid.*
35. MI5 submitted evidence to the ISC that the disclosures by Snowden 'accelerate[d] the use of default encryption by the internet companies... which was coming anyway'. See ISC, *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby* (London: Stationery Office, 2014), para 440.
36. Anderson Report.

> The first concerns real-time court-ordered interception of what we call 'data in motion,' such as phone calls, e-mail, and live chat sessions. The second challenge concerns court-ordered access to data stored on our devices, such as e-mail, text messages, photos, and videos—or what we call 'data at rest.' And both real-time communication and stored data are increasingly encrypted.[37]

The Future: The Internet of Things

1.29 The dependence of society on ICT seems likely only to increase in future, and the advent of cloud computing (the ability to use a network of remote servers hosted on the Internet to store, manage and process data, rather than a local server or personal computer) will mean that digital technology will penetrate every part of the economy and of society.

1.30 The ISR Panel were particularly concerned with the Internet of Things (IoT), as this will have a profound effect on issues of data ownership, acquisition and retention. The IoT refers to a scenario in which everyday products (such as cars, televisions and even clothing) and systems (energy grids, healthcare facilities and transportation systems) are connected to the Internet, allowing them to send and receive data. This is likely to increase the stock of information relating to consumers and their habits and behaviour. One common use already is in wearable technologies such as fitness bands and smart watches. Devices within homes are also becoming connected for energy control and security; smart thermostats, for instance, have the ability to switch a home's heating on or off remotely through the use of a smartphone, and sensors could be used to learn when a user wakes up or leaves the house.[38] The IoT is being driven by the falling cost of sensors, processors and bandwidth. According to a number of reports, it represents a transformative shift for the economy similar to the introduction of the personal computer itself. It also incorporates a number of other major technology-industry trends such as cloud computing, data analytics and mobile communications.[39]

1.31 There are two important implications of the IoT relevant to this review. The first is that the digital society will become more interconnected than ever before: the networked nature of our homes, businesses and public spaces will make the Internet even more pervasive in our daily lives. The second is that the IoT is expected to generate, share and analyse a significant volume of data. While there are a number of different definitions of the IoT, one common factor is the capture and analysis of data in order to deliver some

37. James B Comey, 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?', speech given at the Brookings Institution, Washington DC, 16 October 2014.
38. Ofcom, 'Promoting Investment and Innovation in the Internet of Things: Summary of Responses and Next Steps', Statement, 2015.
39. See for example Dave Evans, 'The Internet of Things: How the Next Evolution of the Internet Is Changing Everything', White Paper, Cisco, 2011; Federal Trade Commission, 'Internet of Things: Privacy and Security in a Connected World', Staff Report, 2015; Ofcom, 'Promoting Investment and Innovation in the Internet of Things'; Vernon Turner et al., 'The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things', Infobrief, International Data Corporation, 2014.

wider benefit. Depending on the application, the data could come from a single device or range of devices. Questions will undoubtedly arise about who owns this data, where it goes, who it is shared with and for what purpose.

The Information Age

1.32 Data is the most valuable commodity of the digital society. The public's use of the Internet has led to an unprecedented supply of information about individuals and their activity, movements and behaviour. Most public- and private-sector organisations in the UK collect and analyse data, albeit to achieve varying ends. In the public sector, data is used by government departments, law enforcement and the SIAs to anticipate and meet social needs, maintain public order, and identify and respond to threats to national security. In the private sector, data can enable companies to be more efficient and respond to market trends and consumer demand. It can also be monetised for marketing and advertising purposes.

1.33 'Data' is a broad term describing a number of different types of information. UK population statistics, an individual's telephone record and the content of a Twitter feed all come under the term 'data' (and will all be of value to different organisations). Data typically takes one of two formats: structured data, where information can be stored and classified in different ways (such as records and fields in a database or spreadsheet); and unstructured data, where information cannot be placed in a tabulated format (particularly from voice, image or video sources). There are a number of terms relating to data that are relevant to this review, particularly in the context of citizen communications.

Personal Data

1.34 Personal data is not necessarily data that a citizen wishes to keep private. Rather, it is defined as data which relate to a living individual, who can be identified from that data or from that data combined with other information which is in the possession of, or is likely to come into the possession of, the data controller.[40] For example, the advent of social media has meant that citizens freely and openly publish personal data about themselves, including visited locations, relationships, photos and contact information. Whether or not data is considered by the individual as genuinely private or sensitive will largely be context-specific.

Big Data

1.35 In recent years societies have seen an exponential growth in data. Some estimates suggest that 90 per cent of all the data in the world has been generated over the last two years. Google processes more than 24 petabytes of data – equivalent to over ninety-six US Libraries of Congress – per day; Facebook has more than 10 million new photos

40. Data Protection Act, Part I, Section I.

uploaded every hour and its users click a 'Like' button or leave a comment nearly three billion times a day.[41]

1.36 The term 'big data' has come to refer to the very large data sets produced in today's digital environment. Data sets are described as 'big' based on a subjective judgement of their volume (the number of fields in the data set), velocity (speed of change of the data set) and variety (types of data in the data set). Whereas traditionally a 'big' data set may have referred to the electoral roll or national telephone directory, today big data refers to large data sets which feature a large number of fields and which evolve rapidly.[42]

1.37 Within this information lie many potentially profitable insights regarding customer behaviour, market trends and supply-chain processes.[43] The rate of data production makes it difficult to analyse using traditional methods, which rely on human analysts distinguishing the most useful information. Over the last decade or so, mathematical tools for analysing large quantities of data and data sets have been developed, which allow computer programmes to run algorithms against the data (at an extremely rapid rate) in order to find correlations.

1.38 In addition to the speed of the analysis, there are numerous advantages to big-data analytics. A large volume and variety of both structured data (for instance, logs of smartphone use within a geographic area) and unstructured data (for instance, sentiment expressed in Twitter feeds) can be analysed simultaneously (perhaps to predict the likely scale and location of riots). Rather than using statistically representative or random sampling, big-data analytics collects and analyses all the data that is available, resulting in a greater degree of accuracy in results.

1.39 Once correlations have been identified, a new algorithm can be created and applied to particular cases. The more correlations that are identified, the more certain kinds of behaviour can be predicted – such as the volume of cars likely to use a new road, the particular consumer goods likely to be purchased by a specific demographic, or even the propensity of an individual to engage in criminal activity.[44]

Communications Data

1.40 As we describe earlier, the term 'communications data' refers to information about an item of communication. According to the Home Office Code of Practice, it refers to 'the "who", "when" and "where" of a communication, but not the content'.[45] For

41. Viktor Mayor-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform the Way We Live, Work and Think* (New York, NY: Houghton, 2013).
42. Information Commissioner's Office (ICO), 'Big Data and Data Protection', 2014.
43. Centre for Economics and Business Research, 'Data Equity – Ireland: Unlocking the Value of Big Data', 2013.
44. ICO, 'Big Data and Data Protection'.
45. Home Office, *Acquisition and Disclosure of Communications Data: Code of Practice* (London: The Stationery Office, 2015), p. 13.

instance, if a call is made between two individuals, the telephone numbers used, duration of the call, and geographic locations of the sender and receiver would all constitute communications data, but not the conversation itself. In relation to Internet communications, the technical identifiers associated with data packets (such as a user's IP address) constitute communications data.

1.41 The existing legislation recognises three types of communications data:[46]

- **Traffic data:** Data attached to a communication for the purpose of transmitting it, and which could identify the sender and recipient of the communication, the location from which and the time at which it was sent, and other related material
- **Service-use information:** Data relating to the use made by any person of a communication service; this is the kind of information that appears on a CSP's itemised billing document to customers
- **Subscriber information:** Data held or obtained by a CSP in relation to a customer; this may be the kind of information which a customer typically provides when they sign up to use a service (for example, the recorded name, address and bank account details of the subscriber of a telephone service).

1.42 CSPs currently retain large quantities of this communications data for internal business reasons (such as customer billing or improvement of services) or to comply with legislative requirements (the set data-retention period of twelve months laid out in the Data Retention and Investigatory Powers Act 2014, for instance). This data can be useful to government, law-enforcement and intelligence agencies – and designated persons within these public authorities can authorise communications data requests from the relevant CSP.

Content Data

1.43 Content data refers to the information which forms the substance of a piece of communication. In comparison to communications data, access to content data has traditionally been thought to be more intrusive, requiring permission in the form of a warrant signed by a secretary of state.[47] As described above, the increasing use of sophisticated encryption methods has made content increasingly difficult to access. CSPs are increasingly anxious to encrypt their content data as a guarantee to customers that it will not be accessed by anyone other than the intended recipient.

1.44 In March 2015, the ISC acknowledged growing concerns over whether the distinction between communications data and content data is still meaningful, and whether changes in technology have meant that access to communications data is now just as

46. Anthony May, *Report of the Interception of Communications Commissioner: March 2015* (London: The Stationery Office, 2015), p. 43.
47. There are circumstances in which content data can be obtained through other means. See, for example, the Regulation of Investigatory Powers Act 2000, s.1(5)(c), s. 3 and 4.

intrusive as access to content data. There are two main arguments as to why this might potentially be the case.

1.45 Firstly, there are greater volumes of communications data available on an individual relative to content data. For every piece of content data (the content of an e-mail, for example) there are multiple pieces of communications data that surround it (the sender and recipient, the time, date, location of transmission and the priority, to name but a few).[48] Communications data is also generated even if no content is ultimately communicated; mobile networks, for example, log the cell location to which a phone is connected even if no call is being made or received.

1.46 Secondly, it is possible to infer a great deal of information from communications data, allowing an analyst to generate a substantial picture of an individual and their patterns of behaviour without ever reading the content of their communications. This can include, for example, examining the location of an individual's phone calls to identify frequently visited locations or examining frequently visited web servers or phone numbers called to reveal details about an individual's private life.

Bulk Data and Bulk Interception

1.47 'Bulk data' is a misleading term as it most frequently refers to the *interception* of data in bulk, rather than to the data itself (hence use of the term 'bulk interception'). Under RIPA 2000, warrants granted under Section 8(4) allow for the collection of communications in large volumes where the sender and/or recipient are located overseas.[49] This bulk collection is done for two reasons. The first reason is to reconstitute split communications; given the nature of how information is transmitted via the Internet – broken down into different packets which are sent over the network and reconstituted at destination – data may need to be intercepted at multiple points in order to understand the whole message. The second reason is to identify unknown threats to national security, or unknown components of previously identified threats (such as members of a terrorist or criminal network, for example), especially overseas. This process is known as 'target discovery', and involves interrogating large volumes of data in order detect or learn more about a particular threat. As described by the ISC:

> GCHQ's bulk interception capability is used primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security. The people involved in those communications are sometimes already known, in which case valuable extra intelligence may be obtained (for example, a new person in a terrorist network, a new location to

48. Written submission from the Information Commissioner.
49. The interception of internal communications, where both the sender and recipient are located within the UK, is subject to tighter controls and more rigorous safeguards than the interception of external communications.

> be monitored, or a new selector to be targeted). In other cases, it exposes previously unknown individuals or plots that threaten our security which would not otherwise be detected.[50]

1.48 A number of the allegations in the Snowden disclosures related to GCHQ's bulk-interception capabilities and tapping of submarine cables, including the TEMPORA and MUSCULAR programmes. The ISC noted that the agency's *access* to bearers is relatively small, but given the scale of *interception*, and the number of citizens whose communications are affected, it considered that bulk 'remains an appropriate term to use when describing this capability'.[51]

Bulk Personal Data Sets

1.49 Large data sets containing personal information about a wide range of people have long been owned and operated by public-sector authorities (examples include the electoral roll, land registry and telephone directory). Most databases containing citizens' health, social security, tax and vehicle records are now computerised. The majority of the public would recognise that this is done for logical and sensible reasons of governance and efficient delivery of services.

1.50 The Driver and Vehicle Licensing Agency (DVLA), for example, maintains a bulk data set containing forty-seven different fields of information about a vehicle. It is primarily used for checking a vehicle is genuine by comparing the make, model, Vehicle Registration Number, and Vehicle Identification Number.[52] More recently, new databases have been created for the purposes of law enforcement. Automatic number plate recognition systems (ANPR) track and store the details of vehicles passing by a camera on major roads and through city centres.[53]

1.51 The legal basis for the acquisition of bulk personal data sets by the SIAs has been cited as the Intelligence Services Act 1994 (ISA 1994) and the Security Service Act 1989 (SSA 1989).[54] The Acts do not explicitly or implicitly address bulk data sets, but they do allow the SIAs to conduct intelligence and security operations which, the SIAs have argued, extends to examining data sets. In March 2015, the use of bulk personal data sets by the intelligence agencies was avowed for the first time.

1.52 Such data sets may be acquired through overt and covert channels. They may be data sets that only the government and its agencies have authorisation to access, such as passport data. The SIAs can also find open-source, bulk personal data sets online, and

50. ISC, *Privacy and Security*, p. 33.
51. *Ibid.*, p. 27.
52. Driver and Vehicle Licensing Agency, 'Bulk Data', V995/1, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/394766/V995X1_090115.pdf>.
53. Home Office, '2010 to 2015 Government Policy: Policing', Policy Paper, 8 May 2015.
54. ISC, *Privacy and Security*, p. 56.

purchase or covertly acquire them, including from overseas as part of the intelligence missions authorised under the ISA 1994.

Data Acquisition, Retention and Access

1.53 There are a number of stages that data goes through between its production and eventual use. It is important to note the various circumstances in which, and processes by which, data is acquired, retained, and eventually accessed and used.

Data Acquisition

1.54 There are a variety of means by which organisations – in both the public and private sector – acquire data. Arguably, the most common method is through citizens voluntarily providing information about themselves. By providing personal data to government services, an individual is able to access a range of services, benefits and opportunities. Examples include NHS health records, passport details and employer information provided to HMRC, to name but a few. In some cases, such as vehicle licensing and house ownership, registration is compulsory. Commercial organisations (both in the UK and overseas) also acquire enormous volumes of information on their customers. Customers may benefit from the collection and analysis of their data by receiving tailored offers, targeted advertising and an overall enhanced retail experience. Consumers are increasingly aware that, although this data was collected for such purposes, it can also be sold or passed onto third parties. Similarly, individuals do not always knowingly, or explicitly, consent to their data being collected or otherwise acquired online.

1.55 One of the most controversial issues in relation to the intelligence agencies and law enforcement is their ability to collect some types of data in bulk. The creation or collection of data sets in this manner is thought by some to be disproportionately intrusive to individual privacy. The UK is not the only country whose intelligence agencies have faced criticism over the collection of communications data in bulk, and the intelligence-collection methods of many nations have come under close scrutiny since June 2013. In January 2014, an inquiry by the European Parliament Committee on Civil Liberties, Justice and Home Affairs reported that there was 'compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data'.[55]

55. Committee on Civil Liberties, Justice and Home Affairs, 'Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs', European Parliament, A7-0139/2014, 2014.

Data Retention

1.56 It is now economically viable for organisations to store data in large volumes for long periods of time, though rarely are we told for how long. Facebook, for example, will store data 'for as long as necessary to provide products and services to you and others'.[56] The long-term availability of such data, and the ability of law-enforcement agencies and SIAs to combine data sets (such as call histories, airline reservations and passport details), makes 'stored data' a valuable source of both evidence and intelligence. Data retention by government is considered by some to be more controversial than retention by the private sector, given that governments have legal and coercive powers over citizens that the private sector does not.

1.57 There are also concerns that data may be retained for the sake of it, under a general justification that it might be of value for as yet unknown purposes at a later date; there is a subsequent risk that it could be held indefinitely and potentially unfairly prejudice an individual in the future. Such arguments were the basis for Part I, Chapter 1, of the Protection of Freedoms Act 2012, which required the destruction of DNA samples and the removal of DNA profiles of certain people in specified circumstances, or those samples which were collected unlawfully or accidentally.

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)[57] 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.[58]

1.59 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 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.[59] Public attitudes to the security of government-held data have been significantly influenced by high-profile media reports over leaks, losses and thefts. In

56. For Facebook's data usage policy see Facebook, 'Data Policy', <https://www.facebook.com/policy.php>.
57. ICO, 'Annual Track 2014: Individuals (Topline Findings)', 2014.
58. ICO, 'Enforcement', <https://ico.org.uk/action-weve-taken/enforcement/>.
59. Ciaran Martin, 'Cyber Security – Sharpening the Focus', speech given at IA14 Conference, London, 17 June 2014.

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.

1.60 European and UK data-protection regulation provides for exemptions for law-enforcement and intelligence agencies to store certain types of data. The ISR Panel were told that only relevant information from stored data is ever released (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).[60] Stored data must be destroyed by the agencies 'as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes'.[61] 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.[62]

1.61 The ICO has advised all organisations that, under the Data Protection Act (DPA) 1998, they should 'identify the minimum amount of personal data you need to properly fulfil your purpose' and should 'hold that much information, but no more'.[63] The Interception of Communications Commissioner's Office (IOCCO) has also undertaken a significant review of the retention, storage and destruction of intercepted material at all the interception agencies. This investigation found that 'every agency has a different view on what constitutes an appropriate retention period for material'. All of IOCCO's recommendations for the SIAs were accepted, leading to a 'significant amount' of material being destroyed. In some circumstances the maximum retention periods for interception and communications data have been halved.[64]

1.62 The SIAs will review the utility of any bulk data set it has acquired (through whatever means) on a regular basis; if there is no reasonable or legitimate reason for keeping the data set, then it will be disposed of. Within MI5, for example, different bulk personal data sets will have a review period of six months, twelve months or two years, depending on the sensitivity of the data within it.[65]

Access to Data

1.63 Businesses can interrogate their own data records at their choosing and use individuals' data based on their consent (for instance, via terms and conditions, T&Cs, at sign up) or another legitimate basis, and pass or sell on this data to third parties – including government, law-enforcement and intelligence agencies. In order for these agencies to access information held by CSPs and ISPs, however, they must go through legally

60. ISR visit to GCHQ, December 2014.
61. See the Regulation of Investigatory Powers Act 2000, Section 15(3).
62. *BBC News*, 'GCHQ "Broke Rules" When Spying on NGOs', 22 June 2015.
63. ICO, 'The Guide to Data Protection', Version 2.2.20, p. 33.
64. May, *Report of the Interception of Communications Commissioner: March 2015*, p. 33.
65. ISC, *Privacy and Security*, p. 58.

established protocols. As already noted, under existing legislation a distinction is made between content data and communications data; access to the latter is generally considered less intrusive under current law, though still requiring the tests of lawfulness, necessity and proportionality to be demonstrated to the authorising officer, a designated person within their organisation, to obtain access. Access to content data is typically granted under a warrant, currently signed by a secretary of state and subject to *ex post* oversight by a commissioner.

1.64 Scarcity of resources and the need to prioritise investigations plays an important part in how data can be analysed by the SIAs and law-enforcement agencies. The ISR Panel were informed by these agencies that the acquisition of bulk data is seen as a means to a specific end, rather than an end in itself. For example, if no initial sources or leads are available, then broad data collection might be undertaken, regarding which context-specific questions would be asked, such as the type of communication device used within a geographic area at a specific time, in order to establish potential leads.[66] The data is then filtered down as much as possible before a human analyst examines it.

1.65 Other search 'selectors' can be applied to narrow the field of data, such as a particular e-mail address, requested from the bulk data set; the agencies operate a process of continually trying to discard false positives and non-threats. The operative process is to narrow down the data funnel to provide useful information and leads.[67] Analysts are not permitted to trawl through data on 'fishing expeditions' as arbitrary intrusion would be unlawful.[68]

The Value of Data

1.66 Modern, democratic governments obtain large quantities of data under their mandate to run public services. There is widespread recognition that data *must* be collected to enable government to govern and in order to ensure the effective management of public services and resources, and that such services are accurately targeted where they are most needed.

1.67 UK citizens have passed much personal data onto the government on a formal basis every ten years since the Population Act (also known as the Census Act) of 1800. In a similar way to the census, the government can use digital information to improve government services (including analysing economic trends, formulating policy and allocating resources to certain activities or geographic areas). The government can also draw on data collected by other organisations.[69] Big-data approaches have been used by all types of public-sector bodies – whether national ones, such as the NHS, trying to

66. ISR visit to GCHQ, December 2014.
67. ISR visit to GCHQ, December 2014.
68. ISC, *Privacy and Security*, p. 45.
69. Katalysis, 'An Open National Address Gazetteer', Department for Business, Innovation and Skills, 2014.

achieve efficiency savings; or local authorities, trying to plan the provision of council services or to model the likely impact of planned buildings, for instance.[70]

Data and Law-Enforcement Agencies

1.68 The digital society has had a significant impact on the police and other law-enforcement agencies. 'Traditional' forms of crime such as fraud are no longer geographically focused; an instance of crime may now have victims across the UK or across many jurisdictions overseas. Criminality has become 'digitally enabled' and law enforcement cannot only respond to this on a purely localised basis. In 2014, Her Majesty's Inspectorate of Constabulary warned that police are 'falling behind the curve of rapidly changing criminality' because of a 'deficit in the skill and experience of investigating officers'.[71] Virtually all investigations today have an online aspect and investigating agencies must have sufficient skills both to establish evidence of criminality, particularly online criminality, and to gather intelligence on potential future threats.

1.69 The increased amount of communications data held by CSPs in recent years has made such information useful as an investigative tool for both security and law-enforcement agencies. In 2014, the home secretary claimed that communications data have been used as evidence in 95 per cent of all serious organised-crime cases handled by the Crown Prosecution Service.[72] Communications data can prove or disprove alibis, identify associations between potential criminals, and can tie suspects to a crime scene. The majority of requests to CSPs for communications data relate to preventing or detecting crime. In 2014, 88.9 per cent of authorisations and notices for communications data by public authorities were made by police forces and law-enforcement agencies.[73]

1.70 In general, law-enforcement investigators will seek to examine communications data as part of their investigations in one of three scenarios:

- The offence has taken place online, meaning the subsequent investigation must also take place online. Volume crimes such as fraud and extortion are increasingly carried out online
- Evidence of an offence has been transmitted via the Internet or by telephone. Telephone records, in particular, are normally examined in relation to individuals in all but the most trivial of criminal cases since they are such a powerful method of indicating (though not necessarily proving) someone's location
- They are interested in the digital footprint of a subject of interest – their recent communications, their acquaintances, recently undertaken journeys,

70. Parliamentary Office of Science and Technology, 'Big Data: An Overview', Postnote, No. 468, 2006.
71. Thomas P Winsor, *State of Policing: The Annual Assessment of Policing in England and Wales 2013/2014* (London: HMIC, 2014), p. 22.
72. Theresa May, *Hansard*, HC Oral Answers to Questions, Col. 456–57 (10 July 2014).
73. Anthony May, *Report of the Interception of Communications Commissioner: March 2015*.

and so on. Even these, however, are increasingly complex to determine. While telecommunications historically went through one single service provider, today the police are interested in communications that go through an ever-growing number of CSPs, hardware and software providers, in addition to applications available on smartphones and tablets. Then, too, online victims and offenders are normally in different geographical locations, if not different national jurisdictions.

1.71 It is worth mentioning that the majority of normal police and law-enforcement work is not concerned with the prevention or investigation of crime as such, but rather with public order and personal safety. Some 70 per cent of all urgent cases to which the Metropolitan Police respond are concerned with vulnerable people – such as missing persons, suicide risks, mental health cases or child abuse.[74]

1.72 The term 'law-enforcement agencies' also includes organisations other than the police. Her Majesty's Revenue and Customs (HMRC), for example, is concerned with law enforcement in carrying out its function to detect tax fraud and evasion. HMRC operates the Connect big-data system that allows it to analyse the majority of its internal data (over 1 billion pieces of data) to find patterns and connections. As of April 2013, HMRC reported that, with an initial investment and five years of running costs of £45 million, it had recovered £2.6 billion through the programme.[75]

Data and the Security and Intelligence Agencies

1.73 While the police and law-enforcement agencies retrospectively seek data as evidence, the UK's intelligence agencies pre-emptively seek data to provide analyses of current national-security issues and to identify future threats. During visits to each of the agencies, it was put to the ISR Panel that communications data has become an essential tool for the police and SIAs.[76]

1.74 The collection of large volumes of information is carried out for target development and identifying new and emerging threats. This involves the SIAs identifying suspects, determining their methods of communication and then selecting their communications data to analyse. This requires positively and reliably associating communications data with specific individuals. Bulk personal data sets are used by the SIAs in three key ways:[77]

- To help identify subjects of interest or unknown individuals who surface in the course of investigations
- To establish links between individuals and groups, or else improve understanding of a target's behaviour and connections

74. ISR Visit to the Metropolitan Police, April 2015.
75. Parliamentary Office of Science and Technology, 'Big Data, Crime and Security'.
76. Theresa May, *Hansard*, HC Oral Answers to Questions, Col. 456–57 (10 July 2014).
77. ISC, *Privacy and Security*, p. 55.

- As a means of verifying information that was obtained through other sources (for example, from human or other signals intelligence).

Data and Industry

1.75 The private sector plays multifaceted roles in regards to data; as creators and generators of data; as victims of breaches, hacks and misuse; and as consumers of data for their own commercial purposes. Collecting and analysing significant volumes of data now forms a key aspect of modern commercial enterprise. Many companies will not allow consumers to access their services without providing certain personal information, while other companies automatically log online activities to generate data on consumer behaviour and spending patterns. One of the first major retailers in the UK to recognise the potential commercial benefits of collecting customer data was Tesco. In return for discounts and offers, the Clubcard loyalty-card scheme proved a useful way for Tesco to track how customers used its services. This model has since been adopted by the majority of large British retailers.

1.76 In many cases, companies outsource the use of big data to intermediary entities, known as data brokers, that collect, analyse and sell consumer information; this may include highly personal details like marital status, religion, political affiliation and tax status. Businesses are able to exploit these vast quantities of data to further their business ends in a variety of ways – from sophisticated market analysis that allows precisely targeted advertising, to tailoring of services for customers and the real-time analysis of financial trends for investment decisions.[78]

1.77 Companies now have the ability to profile and segment customers, based on socioeconomic characteristics, in order to target precisely the people they want to reach. The compilation of consumer databases, which are matched, mined, shared, rented and sold commercially, has become a central feature of business activity.[79]

Conclusion

1.78 As the Internet becomes more integrated into the daily routines of citizens, businesses and governments, the vast amount of digital information produced within our digital society grows at a rapid rate. Some of this data, and the ability to filter and analyse significant volumes of this data, can be immensely valuable to both governmental and commercial organisations. Data has become a commodity to be bought and sold to the extent that many services can be offered to consumers for free.

1.79 Not all uses of data raise dangers to privacy or rights; data analytics to generate insights about large populations are likely to pose relatively less risk than analysis that is aimed

78. ICO, 'Big Data and Data Protection'.
79. House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State. Vol 1: Report* (London: The Stationery Office, 2009), p. 18.

at classifying, sorting or focusing on particular individuals or groups. However, the scale at which data is produced about our activities and behaviour, particularly online, has led to fears that citizens are losing ‘control’ of their data.

II. Privacy and Security

2.1 While the Snowden disclosures may have reinvigorated the ongoing debate on privacy and national security in the UK, it is noticeable that the British public remain largely absent from the debate. The public are regularly asked about their perceptions of the work of the police, SIAs, online privacy and oversight mechanisms, but large portions of society rarely engage with this topic in any great depth.

2.2 The lack of public engagement may in large part be due to the difficulty of navigating these complex issues. Detailed information is often scarce, and discussions are often framed either in abstract terms (the meaning of privacy, the price of security) or in very detailed legal or technical terms (the validity of RIPA 2000 or the implications of end-to-end encryption). Finally, we tend to think of the public and private sectors as two independent spheres of influence and thus fail to spot the obvious similarities and differences in issues of trust, transparency and consent.

2.3 The concepts of liberty, security and privacy are central to a number of universal rights outlined by important pieces of twentieth-century treaties and legislation, including the Universal Declaration of Human Rights 1948, the European Convention on Human Rights (ECHR) 1950 and the UK Human Rights Act 1998.[1] Article 5 of the ECHR sets out a combined right to liberty and security for each person; Article 8 sets out a right to privacy for each person. These rights are not seen as absolute or unconditional, but rather as qualified rights. This qualification – that these rights are in turn subject to other rights – is important if these rights are to be consistent, balanced and mutually reinforcing. Each right must be protected and respected, to the greatest extent possible, but it cannot exist in isolation. 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.

2.4 Following the fundamental Universal Declaration of Human Rights, the international human-rights framework dictates that there cannot be arbitrary interference with these rights. Rights can only be curtailed under certain conditions: firstly, to secure other rights or protect other public interests; secondly, where the consequent restrictions on each right are proportionate; and thirdly, if the specific ways of adjusting rights one to another are lawful. It follows that measures taken by the government to protect rights

1. At the time of writing the government was proposing to replace the Human Rights Act with a British Bill of Rights to 'make our own Supreme Court the ultimate arbiter of human rights matters in the UK'. See Conservative Party, 'The Conservative Party Manifesto 2015', 2015, p. 60.

to personal security will sometimes limit either liberty or privacy (or both) for some. However, the security of the state is not, in itself, a legitimate constraint on the rights of individuals. The security measures taken by states – from surveillance to policing investigation, from data collection to data mining – are legitimate only insofar as they contribute to respecting the rights of persons, such as the right to life.

Privacy

2.5 Like the majority of rights, the right to privacy is a qualified, rather than absolute, right. While everyone has the right to respect of their private and family life, and their home and correspondence, 'a public authority can interfere 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', according to the ECHR.[2] As Anderson notes:

> [The] state has a duty to keep those within its borders safe from criminality. That duty is generally acknowledged to require some ability to intrude upon private communications. Where communication channels are unwatched by the state, and still more when they are incapable of being watched, criminals can act with impunity. That common-sense observation is reflected in the routine activity theory, a criminological staple which states that the three necessary conditions for most crime are a likely offender, a suitable target and – significantly – the absence of a capable guardian.[3]

2.6 The relationship between privacy on the one hand, and liberty and security on the other, is complex. Discussions of privacy and security are often described as a matter of finding or striking a 'balance'; this traditional metaphor can be misleading. There is no metric for 'weighing' different rights, or even for comparing the 'weight' of different rights in particular cases. But it is feasible to set out robust standards that must be met in adjusting rights to one another and to devise and establish structures to do so.

2.7 This framework has come under strain with the emergence of a range of communications technologies that bear on each of these rights and their implementation.[4] In the EU, the informational aspects of the right to privacy are regulated by the Data Protection Directive (1995; subsequently implemented in national jurisdictions), which regulates the use, storage and reuse of personal data, and allows authorised access to such data, recognising that privacy rights must be qualified to allow for rights to liberty and security.

2. Council of Europe, 'Convention for the Protection of Human Rights and Fundamental Freedoms', Rome, 4.XI.1950.
3. David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* [Anderson Report] (London: The Stationery Office, 2015).
4. PR Newswire, 'Digital Divergence: Microsoft Poll Shows Striking Differences in Attitudes Toward Technology between Internet Users in Developing and Developed Countries', 2015, <http://www.prnewswire.co.uk/news-releases/digital-divergence-microsoft-poll-shows-striking-differences-in-attitudes-toward-technology-between-internet-users-in-developing-and-developed-countries-289006871.html>.

2.8 The variety and volume of data we now create daily could be used to damage or violate rights to privacy. But laws and technologies also can be designed in ways that can create boundaries between privacy and security measures. The rights of the person require protection, and thus some form of state law-enforcement and security activity. At both the domestic and the international level, there are strong justifications for providing, by law, the capability for intrusive investigation and surveillance; even those in favour of stronger safeguards for privacy expect to negotiate their level of privacy against other needs in practice.[5]

2.9 Frequent polling and surveys conducted in the UK show respondents, when asked to rank the most serious social issues, cite the NHS, preventing crime, and national security in their top three. Only just over a fifth – 21 per cent – of people asked rank the protection of personal information as a major concern.[6] This should not be taken to mean that British citizens think less of privacy than others, but that their understanding, concerns and feelings about privacy are highly contextual and vary across the UK. Although conceptions of privacy vary, all societies draw some distinction between that which it is conventional and acceptable to do in public and that which is to be kept to a private sphere (whether personal or familial), or in some less-than-fully open context (for example, professional, collegial or commercial confidentiality). Privacy, to use a well-known phrase, is about the 'management of identity', and violations of privacy are seen as leading to vulnerability and to shame. Privacy is an important right because it gives some protection to each individual's ability to control how others see and treat them.

2.10 Privacy is also a pre-requisite for democracy. It gives people the freedom that is needed to be personally autonomous, to seek out alternative sources of information and to question the status quo. Totalitarian states are characterised by their lack of respect for individual privacy, so that citizens are inhibited from voicing any opposition to the state. Those who challenge the state – through journalism or legal advocacy, for example – need to be confident they are not spied upon, otherwise they cannot do their jobs effectively, and such jobs are an acknowledged part of a functioning democracy

2.11 Some – like Mark Zuckerberg, founder of Facebook – have claimed privacy is dead.[7] As technology makes more information more accessible, it also threatens to expose information that is not intended to be shared. However, others in social media – such as Danah Boyd of Microsoft Research – believe people do still care about privacy, and that a big part of our notion of privacy relates to maintaining control over our self-presentation, and that when we do not have that control, we feel that our privacy has been violated.[8]

5. See Introduction in Perri 6, Kristen Lasky and Adrian Fletcher, *Future of Privacy,* Vol 2 (London: Demos, 1998).
6. Information Commissioner's Office (ICO), 'Annual Track 2014: Individuals (Topline Findings)', 2014.
7. Emma Barnett, 'Facebook's Mark Zuckerberg Says Privacy is No Longer a "Social Norm"', *Daily Telegraph*, 11 January 2010.
8. Tony Bradley, 'Privacy Is Not Dead, Just Evolving', PCWorld, 14 March 2010, <http://www.pcworld.com/article/191506/Privacy_is_Not_Dead_Just_Evolving.html>.

This concept of control is increasingly important to citizens and consumers alike. The number of users of social-media platforms continues to grow at a rapid rate, as more and more people seek to share information online. Yet 45 per cent of the population say they feel they have little or no control over the personal information companies gather about them while they are browsing the Web or using online services, such as photo-sharing, travel or gaming.[9]

2.12 It is therefore unsurprising that citizens may seek to regain control over information available about themselves online by exercising a 'right to be forgotten', particularly if this information is inaccurate. Not everyone wants to have their information online for all to see. A May 2014 judgment of the Court of Justice of the EU ruled that Google had to 'adopt the measures necessary to withdraw personal data [relating to the claimant] from its index and to prevent access to the data in the future'.[10] The 'right to be forgotten' was thus enshrined in European law, granting all EU citizens the right to request search engines to remove links to personal information about them online, under certain conditions. The ruling was based on the 1995 Data Protection Directive and Articles 12 (Right of Access) and 14 (Right to Object) in particular, which state that a person can ask for personal data to be deleted in certain circumstances. Since Google launched its official request process, it has received 32,192 requests from the UK to remove 127,004 URLs. Of these, Google has so far removed 39,646 URLs (37.6 per cent).[11] The law applies regardless of the individual's nationality and even if the physical server of the company is located outside of Europe: 'EU rules apply to search engine operators if they have a branch or a subsidiary in a Member State which promotes the selling of advertising space offered by the search engine'.[12] However, this does not require the company to destroy the data, and Google is free to list a removed search result on their US or other non-European websites. Thus, a search of google.com in the US will reveal data that google.co.uk has had to remove for UK or European searches.

2.13 Any intrusion into people's lives therefore needs to comply with various legislation, including Data Protection law, Article 8 of the European Convention of Human Rights and, of increasing significance, Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Any processing by government of personal data, including the collection of data and access to stored data, needs to be necessary, proportionate and justified, with effective oversight arrangements in place.

9. Microsoft, 'Survey Shows People Need More Help Controlling Personal Info Online', News Centre, January 2013, <http://news.microsoft.com/2013/01/23/survey-shows-people-need-more-help-controlling-personal-info-online/>.
10. European Court of Justice, 'Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González', C-131/12 ruling, point 2.
11. Correct at the time of writing. See Google, 'European Privacy Requests for Search Removals', Transparency Report, <http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en>.
12. European Commission, 'Factsheet on the "Right to be Forgotten" Ruling', C-131/12, 2014.

2.14 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.[13] 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'.[14] 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.

Why Privacy Matters

2.15 Privacy protects a set of deeply significant values that no society can do without; it is about the lines, boundaries and relationships we draw between and among ourselves, communities and institutions. Rather than an empty ideal or state, attitudes towards privacy tell us much about those fundamental relationships; what people think and expect of their neighbours, their fellow citizens and their government.[15]

2.16 The most striking characteristic of public discussions on surveillance to date is the perceived dichotomy between the rights or values of collective security and privacy. A common and repeated assumption made by politicians, the media and the general public is that these values are opposed, and that the issue is one of 'national security' *versus* 'personal privacy'. The subsequent assumption is that a trade-off can be made between the two: Is the right balance being struck between national security and civil liberties, or between collective security on the one side and individual freedoms and personal security on the other?

2.17 There is also a tendency to want both maximum security and privacy simultaneously. Desires for one or the other change according to how they are defined and how they apply to specific circumstances:

> People do care about their privacy. They also care about security, but they define it in many different ways. As has been discussed, privacy is a very complex concept with many facets,

13. Written evidence to the ISR from the Office of the Information Commissioner, Christopher Graham.
14. *The Economist*, 'Data, Data Everywhere', 25 February 2010.
15. Charlie Edwards and Catherine Fieschi (eds), *UK Confidential* (London: Demos, 2008).

> and exercised in many domains. Likewise, security is not a very clear concept, much less national security.[16]

2.18 A second common aspect of public attitudes towards data and surveillance is a deficit of trust and confidence in institutions. Private-sector companies seem to know more about their users every day, and more personal information appears to be moving online. At the same time, a significant portion of the public has doubts of the proper conduct of the government via its security and law-enforcement agencies.

2.19 Prior to June 2013, when information provided by Snowden was first disclosed, people were already aware that they may not be in complete control of their data when online. The allegations over GCHQ's TEMPORA programme and its interception of communications via submarine fibre-optic cables were criticised as 'surveillance on an industrial scale' and 'quite simply, the largest violation of the right to privacy in British history'.[17] On the other hand, the ISC has argued that the disclosures have led to 'allegations, myths and misconceptions about the Agencies and these have damaged... trust'.[18]

2.20 For members of the public, it can be hard to reconcile confidence and trust in the police and SIAs with phrases such as 'mass interception', 'snoopers' charter' and 'bulk collection'. This is why popular perceptions of public attitudes may seem disjointed. People expect the police to be able to use bulk data interception techniques to track down missing persons, but do not like thinking about their own data in the hands of the police or the intelligence agencies. We do not want personal information to be used and sold without our consent, yet often accept T&Cs without reading them first, or voluntarily hand over personal information in exchange for free services.

2.21 In general terms, public attitudes towards the agencies, and towards data, privacy and surveillance, have proved ambivalent since June 2013. The public debate over surveillance has not been as pronounced or as animated as in some other countries. Collectively, we may express worry or dissatisfaction about 'bulk data interception' while individually supporting enhanced capabilities for the security and intelligence services to keep us safe.

Perceptions of Data Privacy

2.22 As the market-research organisation Ipsos MORI itself points out, 'there is no one public opinion on data privacy'.[19] In analysing the results of various polls, studies and surveys conducted over the last three years, there is significant variation in public awareness of

16. Charles D Raab, uncorrected submission of evidence to the ISC Privacy and Security Inquiry, Public Evidence Session 3, 7 February 2014.
17. Don't Spy on Us, 'Don't Spy on Us: Reforming Surveillance in the UK', 2014, p. 4.
18. Intelligence and Security Committee of Parliament (ISC), *Privacy and Security: A Modern and Transparent Legal Framework* (London: The Stationery Office, 2015), p. 107.
19. Ipsos MORI, 'Understanding Society: The Power and Perils of Data', 2014, p. 2.

how data is collected, used and shared; in public understanding of the parameters of the debate; and in how concerned different people are by threats to their personal privacy. These concerns are also specific to each situation – people do not tend to simply make a general 'trade-off' between privacy and security – and opinions can change depending on different data use, data users and data purposes.

2.23 Polling also shows that, while people may be concerned in general terms, data-privacy issues are not at the forefront of their thoughts, and their behaviour may not reflect stated levels of concern. Indeed, Ipsos MORI notes that 'stated concern about data privacy and how people actually behave are barely nodding acquaintances'.[20]

2.24 There is reason to suspect that the British public are most concerned by data collection and use by the private sector. According to the 2014 UK TRUSTe Privacy Index, 20 per cent of those who said they were concerned by online privacy said that this was caused by reports of government surveillance; 60 per cent were concerned as a result of businesses sharing personal information with other companies.[21] While about one in five adults (19 per cent) in the UK feel that consumer experiences are being enhanced by big companies gathering large amounts of their personal data for internal use, almost half (46 per cent) feel that consumers are being harmed.[22]

Security

2.25 In the 2010 National Security Strategy, the first such comprehensive strategy in the UK, the government noted that 'The security of our nation is the first duty of government. It is the foundation of our freedom and our prosperity'.[23] Implicit in this statement is that the ability of the public to exercise a number of their fundamental rights – including the right to privacy, freedom of expression and *individual* security – is dependent on well-regulated forms of *state* or *national* security. Individual security and collective security are therefore closely linked, and in order to enjoy our rights and freedoms there is a public expectation that government, through its law-enforcement agencies and SIAs, will ensure public safety and protect us from a range of different threats.

2.26 According to the 2010 National Security Strategy, Britain faces a complex range of threats from a myriad of sources including terrorism, organised crime, cyber-attacks and unconventional attacks using chemical, nuclear or biological weapons. The security of the UK's energy supplies depends on fossil fuels located in some of the most unstable parts of the planet. Nuclear proliferation is a growing danger. British security is vulnerable to the effects of climate change and its impact on food and water supply. These threats are

20. *Ibid.*, p. 3.
21. TRUSTe, 'TRUSTe Privacy Index', 2014 UK Consumer Data Privacy Study, <https://www.truste.com/resources/privacy-research/uk-consumer-confidence-index-2014/>.
22. Big Brother Watch, 'UK Public Research – Online Privacy', 2015, p. 3.
23. HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (London: The Stationery Office, 2010), p. 9.

often framed as not just diverse but, in an age of rapid globalisation and extensive cross-border travel, increasingly international. They can also develop and diminish rapidly; in the five years since the National Security Strategy was published, a range of global events continue to demonstrate this volatility; as Sir John Sawers, former chief of SIS expresses it, 'we have to anticipate, discover, analyse, investigate and respond, and we have to do it globally because the threats are coming at us globally'.[24]

2.27 These new threats can emanate from states and non-state actors and often manifest themselves in frequent, lower-level and less-sophisticated attacks, which are much harder for intelligence agencies to detect and disrupt. In addition to the murder of Lee Rigby in Woolwich in 2013, so-called 'lone actor' terrorist attacks over the course of the last two years in Copenhagen, Ottawa, Paris and Sydney are examples of this type of threat. The attack by a lone individual on British tourists in Tunisia in June 2015 caused the highest number of British casualties since the attack on the London transport system in 2005.

2.28 The terrorist threat is diverse and takes a number of different forms – from Islamist to extreme right-wing ideologies, and from established groups to self-organised individuals ('spontaneous and volatile extremists'). At the time of writing, the threat level for terrorism in the UK is Severe and is strongly influenced by British nationals returning to the UK having fought in the Syrian civil war, the scale of which, in terms of the number of British foreign fighters, is unprecedented. Given the diversity of the terrorist threat, the police and SIAs have all had to adapt their approach and capabilities. MI5, for example, has experienced a substantial period of growth and the organisation is double the size it was at the time of the 2005 London bombings.[25]

2.29 The Internet is already used by terrorists to spread propaganda, radicalise potential supporters, raise funds, communicate and plan attacks. While terrorists can be expected to continue to favour high-profile physical attacks, the threat that they might also use the Internet to facilitate or to mount attacks against the UK is growing.[26] The influence of the Islamic State of Iraq and the Levant (ISIL) is spreading and social media is a useful propaganda tool for the organisation, particularly in encouraging lone actors. The director of GCHQ described the array of threats, and the degree to which terrorists and criminals are using technology to their benefit, in more stark terms in the *Financial Times.* He wrote that technology companies 'have become the command-and-control networks of choice for terrorists and criminals, who find their services as transformational as the rest of us.'[27]

---

24. Evidence submitted at the ISC open evidence session, 7 November 2013.
25. To provide a comparative scale, however, the scale of their operations remains just 1 per cent of that of the East German Stasi in terms of GDP per capita.
26. Cabinet Office, 'The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World', 2011.
27. Robert Hannigan, 'The Web is a Terrorist's Command-and-Control Network of Choice', *Financial Times*, 3 November 2014.

2.30 The threat too from organised crime to the UK is growing. A recent Europol assessment suggested that the Internet and communications technology has created a professional, continually evolving, service-based criminal industry which 'drives the innovation of tools and methods used by criminals and facilitates the digital underground through a multitude of complementary services, extending attack capacity to those otherwise lacking the skills or capabilities'. It also highlights the risk of online marketplaces and fora, which 'provide cybercriminals with a nexus for the trade of goods and services and a hub for networking, creating an organised set of criminal relationships from an otherwise disparate population.'[28]

2.31 The UK's Cyber Security Strategy outlines the growing and dynamic threat, from states and non-state actors via the Internet and communications technology, to steal, compromise or destroy critical data. As the strategy makes clear, the scale of the UK's dependence on the Internet means that its prosperity, key infrastructure, places of work and homes can all be affected.[29]

2.32 The use of ICT in espionage represents another important aspect of the threat. As the Anderson Report notes, 'Cyber espionage allows information to be stolen remotely, cheaply and on an industrial scale at relatively little risk to the hostile state's intelligence officers or its agents'.[30] This not only affects the government and its agencies – the intellectual property of UK companies are just as much of a target.

Perceptions of the Agencies

2.33 The public's support for legitimate state law-enforcement and security and intelligence work is crucial, and the police and SIAs themselves are the first to acknowledge that they require public consent – it underpins their licence to operate. Even if it is universally accepted that the agencies must keep some operational details of their work secret, the public must support in principal what the agencies do and be confident they are acting within a legal framework. The public must also remain confident in the accountability and oversight mechanisms which verify that the agencies are operating within justifiable moral, ethical and legal limits, and their work carried out in the public interest. In the words of the ISC, 'There is a legitimate public expectation of openness and transparency in today's society, and the intelligence and security Agencies are not exempt from that'.[31] While almost four in five adults (79 per cent) in the UK are concerned about their privacy online,[32] they also appear – for the most part – to be supportive of the agencies (see Figure 2).

28. Europol, 'Key Findings', The Internet Organised Crime Threat Assessment (iOCTA), 2014, <https://www.europol.europa.eu/iocta/2014/keyfindings.html>.
29. HM Government, 'The UK Cyber Security Strategy', Annex 10.
30. Anderson Report, p. 44.
31. ISC, *Privacy and Security*, p. 2.
32. Big Brother Watch, 'UK Public Research – Online Privacy', p. 2.

Figure 2: 'Do you think the British security services (such as MI5) have too many powers to carry out surveillance on ordinary people in Britain, too few powers to carry out surveillance, or is the balance about right?' (%)

Source: YouGov

2.34 This is further supported by a YouGov poll of January 2015 which asked whether the public thought the security services did or did not need more access to the public's communications (such as e-mails and phone calls) in order to effectively fight terrorism. The majority (52 per cent) believed they did need more access, compared to 31 per cent which believed that they already have all the access they need or more than they need, while 17 per cent did not know.[33]

2.35 Overall trust in the SIAs also appears to be high, even when compared to the police. In the same YouGov poll, 63 per cent of respondents said they would have trust in the intelligence services to behave responsibly with information obtained using surveillance powers, compared to 29 per cent who said they would not have trust. For the police, 50 per cent claimed they would trust the police to behave responsibly, compared to 42 per cent who said they would not have trust.[34]

Perceptions of Oversight

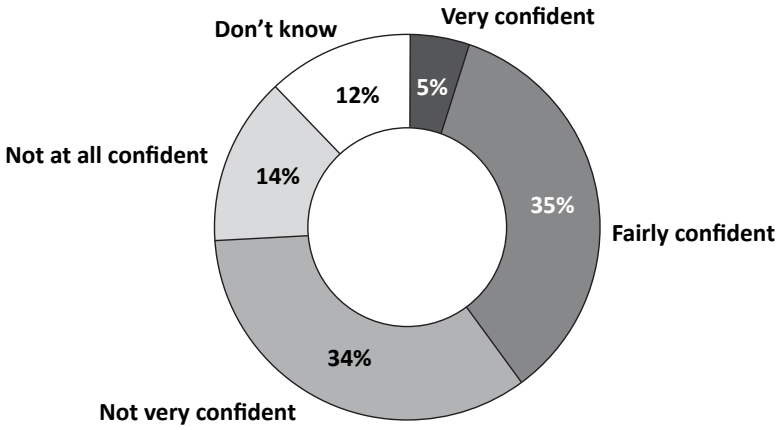
2.36 A further significant concern of some portions of society, and of privacy and civil-liberties groups in particular, is that there is insufficient oversight of the SIAs, and that they are free to set their own mandate. The agencies, they fear, are 'left virtually unconstrained and unsupervised by out-dated legislative frameworks, [and] have unilaterally expanded the scope of their activities and the extent of their capabilities'.[35]

2.37 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

33. YouGov/*Sunday Times*, 'Survey Results', 15–16 January 2015, <https://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/wt26kxdn72/YG-Archive-Pol-Sunday-Times-results-160115.pdf>.
34. *Ibid.*
35. Don't Spy on Us, 'Don't Spy on Us: Reforming Surveillance in the UK', p. 10.

these agencies'.[36] These criticisms over its membership, outputs and degree of independent scrutiny have contributed to the deficit in public confidence, as illustrated by an Ipsos MORI survey from May 2014, shown in Figure 3.

Figure 3: 'Currently, the UK's intelligence agencies are held to account on behalf of the public by a committee of politicians. How much confidence, if any, do you have in the current system of holding the intelligence agencies in the UK to account?'



Source: Ipsos MORI

2.38 Oversight through elected representatives is an essential principle in a democracy, and the Committee is intended to be an important vehicle for transparency. However, as a result of the criticisms outlined above, the public perception is that politicians – who do not tend to score highly in surveys gauging public trust of various professions – are not best placed to provide oversight of the agencies.

2.39 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'.[37] Evidence submitted to the ISR Panel suggests that the commissioners and their work are not well known among the general public, and the role of the expert inspectors who support them is equally underappreciated by their critics.

36. *Ibid.*, p. 25.
37. *Ibid.*, p. 27.

The Public's Awareness of Data Collection and Use

2.40 It is reasonable to suggest that the public's perceptions of surveillance, the agencies and oversight outlined above would change if they were more aware of some of these issues and, in particular, if they were aware of how much of their data is collected and used.

2.41 As noted also in Chapter I, the public do not fully appreciate the scale of data collection in our digital society. Much of this data collection occurs without us even realising it. People unwittingly give away information when they use smartphones; buy things via PayPal on eBay; post content on Facebook or Twitter; and use Internet search engines, all of which can be tracked and analysed and the data sold on the open market.[38]

2.42 One of the primary reasons given by those polled for discomfort with the collection of data is a sense that it has been carried out without explicit, informed consent. When subscribing to services offered by private-sector companies, users are presumed to provide consent by agreeing to T&Cs. To be considered acceptable under the DPA 1998, the processing of information has to be fair and lawful. In its guide to data handlers, the Information Commissioner's Office stresses that 'fairness generally requires [users of data] to be transparent – clear and open with individuals about how their information will be used'. It argues that people should have the means to 'make an informed decision' about 'whether to enter into [the] relationship'.[39]

2.43 The methods used to seek consent in online transactions are often less demanding than those used in certain other areas. In clinical medicine and biomedical research, for example, requirements for informed consent are taken more seriously, and standards are set out in professional and regulatory requirements. One example of an area where informed consent is considered to be particularly important is that of medical records and health data. Although not stored centrally, the NHS holds millions of cradle-to-grave records of citizens and significant volumes of health-related data. Polling suggests that we trust health workers (doctors) more than other public figures with our personal data. Most would agree that analysing this data can be very helpful for both diagnosis and health management.[40] However, there is a risk that consent to the use of medical records in commercial contexts may be subject to 'ticking and clicking' without reading, let alone understanding, the T&Cs or other content to which consent is ostensibly given. Data subjects – whether patients or research participants – cannot be expected to understand large amounts of medical or other technical information of high complexity, or to grasp all of the ways in which data that pertain to them could be reused. In other words, they

38. The Ditchley Foundation, 'Intelligence, Security and Privacy', conference terms of reference, 14–16 May 2015, <http://www.statewatch.org/news/2015/may/uk-ditchley-intelligence-and-security-conference.pdf>.
39. ICO, 'Processing Personal Data Fairly and Lawfully', Guide to Data Protection, <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/>.
40. Parliamentary Office of Science and Technology, 'Big Data and Public Health', Postnote, No. 474, 2014.

cannot give fully explicit or specific consent to uses of data that they do not, indeed cannot, understand. And with the development of 'e-health', ever-greater volumes of personal lifestyle data are being produced by consumers using wearable technology devices. For example, using in-built sensors in iPhones, Apple's ResearchKit open-source software framework lets researchers create apps to 'gather new types of data on a scale never available before'.[41] In these circumstances, there is even less clarity for the user over how their data will be used and repurposed by these commercial entities.

Figure 4: Word Length of Terms and Conditions of Popular Internet Services.[42]

Website/Service	Total Words
PayPal	36,275
Hamlet	30,066
Apple iTunes	19,972
Macbeth	18,110
Windows Live	14,714
Apple iOS 5	13,366
Facebook	11,195
Google All-Inclusive	10,640
Apple iCloud	10,724
Amazon Kindle	7,115
Amazon.co.uk	5,212
Twitter	4,445

2.44 In order to collect data on their customers, commercial organisations must seek permission from users to do so. However, some argue that agreeing to terms is not evidence of explicit, informed consent. Many will hastily agree to T&Cs as they are eager to unlock the opportunities that agreeing to them offers. For example, an experiment into the dangers of public WiFi use in 2014 saw six users agree to T&Cs requiring them to give up their first-born child in exchange for free WiFi.[43] T&Cs and privacy agreements can often be extremely lengthy and written in legalistic language (see Figure 4); this makes it difficult for the user to fully understand how his or her data will be collected and used. A report commissioned by Belgium's National Data Protection Authority[44] concluded that Facebook's revised T&Cs gave users a false sense of control over their

41. Apple, 'ResearchKit', <https://www.apple.com/uk/researchkit/>.
42. Rich Parris, 'Online T&Cs Longer Than Shakespeare Plays – Who Reads Them?', Which? Conversation, 23 March 2012, <http://conversation.which.co.uk/technology/length-of-website-terms-and-conditions/>.
43. Tom Fox-Brewster, 'Londoners Give Up Eldest Children in Public Wi-Fi Security Horror Show', *Guardian*, 29 September 2014.
44. Brendan Van Alsenoy et al., 'From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies', draft version 1.2, 2015, <http://www.law.kuleuven.be/icri/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf>.

data privacy and was in violation of European privacy law.[45] A follow-up report[46] found that Facebook could track users across the Internet without their consent, even if they were not logged into Facebook at the time.[47]

2.45 In May 2015 the ICO announced a review of websites and apps used by children into the type of personal information that may be collected, and will consider whether legal action should be brought against any website or app found to be breaking the DPA 1998.[48] The use of online services and apps by children is often unsupervised by adults and therefore they may be particularly vulnerable to inadvertent data collection.

Public- and Private-Sector Transparency

2.46 While there have been calls demanding greater levels of government and agency transparency – directly or via the commissioners and ISC – there have also been calls for industry to be more transparent in how and when they collect and share data. Periodic transparency reports, such as those published by Google,[49] Vodafone[50] and Facebook[51] illustrate the response of private-sector companies to these calls.

2.47 Public understanding of surveillance for law-enforcement and intelligence purposes, and the way in which personal data is processed, must therefore involve a certain degree of organisational transparency. This transparency must apply at every stage of the process, from the early stage of government setting its priorities for intelligence collection, to information from the SIAs on the ways in which they acquire and retain information, through to the audit processes implemented by the ISC and the commissioners.

2.48 That is not to say that all intelligence activity by the police and SIAs should be transparent. Revealing sources and methods simply enables criminals and adversaries to evade attention, impairing intelligence operations. In an area such as national security, where there are obvious sensitivities around revealing capability gaps, there is understandable hesitation from government and the agencies to provide information on capabilities and

45. Stephen Fidler, 'Facebook Policies Taken to Task in Report for Data-Privacy Issues', *Wall Street Journal*, 23 February 2015.
46. Güneş Acar et al., 'Facebook Tracking Through Social Plug-ins', version 1.1, 2015, <https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf>.
47. Samuel Gibbs, 'Facebook "Tracks All Visitors, Breaching EU law"', *Guardian*, 31 March 2015.
48. ICO, 'ICO Launches Review of Children's Websites and Apps', News, 11 May 2015, <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/05/ico-launches-review-of-childrens-websites-and-apps/>.
49. Google, 'Access to Information', Transparency Reports, <http://www.google.com/transparencyreport/>.
50. Vodafone, 'Sustainability Report 2013/14', <http://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf>.
51. Facebook, 'Global Government Requests Report', <https://www.facebook.com/about/government_requests>.

processes. However, the ISC itself acknowledges the importance of providing the public with information, particularly on standards and safeguards:

> We recognise that much of the Agencies' work must remain secret if they are to protect us effectively. However, given that their work may infringe ECHR rights such as privacy, we consider it essential that the public are given as much information as possible about how they carry out their work, and the safeguards that are in place to protect the public from unnecessary or inappropriate intrusion.[52]

2.49 It is true that the agencies are more open today than ever before. This has been a gradual process since they were publicly acknowledged in the late 1980s and early 1990s. As part of an increasing range of outreach activities, eighty GCHQ employees currently publicly identify themselves. From next year, more GCHQ information and guidance will be published online as part of their public-facing security mission. Former editor-in-chief of *The Guardian* newspaper, Alan Rusbridger, has noted that GCHQ in particular has become more open to the press: 'there has been a great deal of "opening up" and that is to the agency's credit'. [53] The publication of an article written by the current director of GCHQ in November 2014 has been cited as an illustration of this.[54]

2.50 Nevertheless, there have been calls from those who believe that the agencies can be yet more transparent about some aspects of their work. The Open Rights Group, for example, has called for the government to publish 'aggregate information on the number of surveillance authorisation requests approved and rejected so that citizens can understand the scale of surveillance requests made by the intelligence agencies and by government agencies'.[55] Information relating to the SIAs, including their communications, is currently exempt from requests under the Freedom of Information Act (FOIA) 2000.

2.51 Many NGOs, such as Open Rights Group, Liberty, Privacy International, Big Brother Watch and Index on Censorship, have joined forces to run high-profile campaigns, such as Don't Spy on Us. They have also launched joint legal proceedings; in 2014, Privacy International, Liberty and Amnesty International took a case to the IPT, requesting that the court review the legality of, and policy regime relating to, the PRISM programme and the lawfulness of interception by the security services. The IPT in February 2015 found in favour of GCHQ in terms of proportionality and necessity but, importantly, found that the government had not adequately explained (to the extent required by the Human Rights Act) the safeguards for domestic communications intercepted incidentally during foreign-intelligence gathering. In response, the NGOs have launched an appeal at the European Court of Human Rights (ECtHR), challenging the UK government's surveillance of data.

52. ISC, *Privacy and Security*, p. 16.
53. Alan Rusbridger, speech given at RUSI, London, 19 January 2015.
54. Robert Hannigan, 'The Web is a Terrorist's Command-and-Control Network of Choice'.
55. Don't Spy on Us, 'Don't Spy on Us: Reforming Surveillance in the UK', p. 8.

2.52 In June 2015, a report by Big Brother Watch used police data obtained using the FOIA 2000 which showed officers were making a request for communications data every two minutes and obtaining access in 96 per cent of cases. In a response to the report, the Office of the Interception of Communications Commissioner (IOCCO) highlighted the fact that much of the police data contained in the report was collected under older – and flawed – statistical requirements, and that some of Big Brother Watch's recommendations were now implemented.[56]

2.53 A particular concern of the ISR Panel is that surveillance and mass data collection by private-sector organisations is largely overlooked in discussions of transparency. The acquisition, retention and use of citizen data by the private sector is a crucial aspect of the debate, which needs to be addressed.

2.54 Bearing in mind the multitude of opinions and arguments over privacy, ethics and human rights, the Panel note that much of the significant controversy over the interception of citizens' data revolves around three key questions: Are the public aware of who can collect their data and for what purpose? Do the public have confidence in the legislative and governance frameworks which govern data usage? Are the public satisfied with the authorisation, accountability and oversight checks that are in place?

56. Interception of Communications Commissioner's Office (IOCCO), 'Why Policy Makers Should Exercise Caution with the Communications Data Figures Published in the Guardian's Article Today Claiming That Requests Are "Out of Control" Via Big Brother Watch', 2015, <http://www.iocco-uk.info/docs/Response%20to%20the%20Guardian%20article%20of%201st%20June%202015.pdf>.

III. Challenges for the Police, Security and Intelligence Agencies

3.1 Chapter I describes the impact of the Internet and communications technology on British society and both the challenges and benefits of becoming a digital society. In a recent speech, Baroness Lane Fox of Soho, a member of the ISR Panel, suggested that 'It is within our reach for Britain to leapfrog every nation in the world and become the most digital, most connected, most skilled, most informed on the planet.'[1] Many would subscribe to this vision, especially as the benefits of the digital era are increasingly apparent. But we must also accept that in becoming the most digital and connected nation on the planet there are costs and implications for our collective security and individual privacy – firstly, as more of our personal and sensitive data is sent out across the Internet and, secondly, as criminals, foreign governments and terrorists discover ever-more sophisticated ways to exploit this.

3.2 The police and SIAs have had to adapt their strategy and approach to the digital era, a change neatly summed up in a speech by Baroness Smith of Basildon, shadow leader of the House of Lords:

> Some people may look back with nostalgia to the Cold War, but the days when a man in a gabardine mac and a trilby kept watch while his colleague unscrewed the telephone to install a bug and hide a microphone in the plant pot have long gone. Those involved in terrorism, or in serious and organised crimes like drug and people trafficking, international fraud, hard core pornography, paedophilia and child sexual abuse, do so today with a sophistication and technical knowledge that many of us would struggle to comprehend.[2]

3.3 The disclosures by Edward Snowden exposed some of this new tradecraft in 2013. These raised a number of issues, including: the scale of the threat facing the UK from foreign governments, terrorist organisations and criminals; the response by the police and the SIAs to these threats; and the legislation that governs their actions. The disclosures also raised serious questions about the oversight and accountability regime in the UK. The ISR Panel was tasked with advising on the legality, effectiveness and privacy implications of the UK surveillance programmes and also to make an assessment of how law-enforcement and intelligence capabilities can be maintained in the face of technological change, while respecting principles of proportionality, necessity and privacy. The legality of the programmes has been considered, including by the IPT, which has concluded that

1. Martha Lane Fox, speech delivered at the 2015 Richard Dimbleby Lecture, 30 March 2015.
2. Baroness Smith, *Lords Hansard*, Daily Hansard, Col. 305 (2 June 2015).

the powers of the agencies are being used lawfully. Legal challenges at the European Court of Human Rights are ongoing.

3.4 As the UK has become one of the most connected and data-rich countries, the government and the private sector have gradually constructed one of the most extensive and technologically advanced digital-intelligence systems in the world. While the ISR Panel did not consider the entire range of capabilities accessible to the SIAs, we focused on some of the key issues highlighted by Snowden's disclosures. Given the exponential growth in data and the ubiquity of communications technology, we also considered the impact this had on the police, NCA as well as the UK's three security and intelligence agencies. To that end we visited GCHQ, the NCA, the Metropolitan Police, the Security Service (MI5) and the Secret Intelligence Service (SIS).

3.5 On the whole, the ISR Panel found it challenging to reconcile the disclosures made by Snowden with the oversight systems and processes outlined by the organisations visited. What was apparent was that in the past neither the government nor the overseers had felt it necessary to provide information about how the law regarding interception was actually being applied in practice. As a result, these processes were not well understood by politicians or the wider public, which made the media's allegations of wrongdoing all the more powerful.

3.6 The ISR Panel were also struck by the scale of the challenge facing the police, NCA and SIAs in this new digital era. In this regard, the development by the College of Policing, NCA and National Police Chiefs' Council of a framework for Digital Investigation and Intelligence is welcome. However, it is also overdue. The police in particular are struggling to meet the challenge today – let alone develop an approach for the future. The challenges facing the police from the growth in digital communication include:

- An increasing volume of crime being committed online
- The Internet providing significant new opportunities for investigation
- The continuing need to investigate 'traditional' crimes but with fewer resources
- The need to ensure staff are knowledgeable about and trained in digital technologies.

The Snowden Disclosures

3.7 This is the landscape in which the disclosures of classified intelligence material by Edward Snowden first appeared in newspapers in June 2013. Snowden, an American computer specialist, was formerly an employee of contractors to the NSA. In May 2013, he disclosed to journalists details of covert US intelligence and surveillance programmes. Estimates of the number of files Snowden removed from the NSA without authorisation range from the hundreds of thousands to 1.7 million, though there are no agreed figures. The

ISR Panel understand that 58,000 of these classified files relate to GCHQ and UK security and intelligence activity.[3]

3.8 The allegations made in the wake of the Snowden disclosures covered a range of intelligence activities – though they were primarily concerned with the activities of the NSA, given the closeness of the intelligence relationship between the US and UK, they also covered many of the activities of British SIAs, particularly the work of GCHQ. The British government has maintained its policy of neither confirming nor denying these allegations; although the PRISM programme was avowed by the US government.[4]

3.9 Snowden's disclosure of the NSA programme that collected data on the communications of US citizens (under Section 215 of the USA Patriot Act) created public anger in many quarters in the US towards the federal government and the NSA on the grounds that the programme violated the Fourth Amendment of the US Constitution prohibiting unreasonable searches, and has led to congressional efforts to constrain the NSA's operations. More than twenty legislative bills have been written since the NSA allegations began, many with the goal of clarifying US government surveillance powers. The NSA's phone-spying programme was ruled illegal by a US appeals court in May 2015,[5] ultimately leading to significant reform under the USA Freedom Act. Enacted in June 2015, the Act imposes new limits on the bulk collection of communications data on US citizens by US intelligence agencies and requires US CSPs to collect and retain communications data (similar to the current situation in the UK).

3.10 While the majority of the disclosures made by Edward Snowden relate to surveillance practices in the US, they also allege that GCHQ were tapping fibre-optic cables carrying vast amounts of global communications and sharing data with the NSA.[6] *The Guardian* newspaper suggests that the existing UK legislation was being very broadly applied, and in ways the public were unaware of, to allow digital-intelligence operations on a large scale.[7]

3.11 Representatives of *The Guardian* informed the ISR Panel that, out of the twelve main stories based on the information provided by Snowden, only one was published without notifying GCHQ beforehand. Its then editor-in-chief, Alan Rusbridger, made the newspaper's position clear: there was an important public interest in revealing the scale of surveillance and its implications for privacy, but that the paper would not, after taking expert advice, publish information it believed would put intelligence officers in danger

3. Oliver Robbins, 'First Witness Statement of Oliver Robbins', statement to the High Court, CO/11732, 27 August 2013.
4. Privacy and Civil Liberties Oversight Board, 'Report on The Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', 2014.
5. *Reuters*, 'NSA's Phone Spying Program Ruled Illegal by Appeals Court', 7 May 2015.
6. Ewen MacAskill et al., 'GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications', *Guardian*, 21 June 2013.
7. *BBC News*, 'Edward Snowden: Leaks That Exposed US Spy Programme', 17 January 2014.

or prejudice the security of the public.[8] Some note that journalists and media outlets thereby acted as 'risk analysts', or as filters for the material, to avoid a similar 'data dump' as was the case with WikiLeaks. Others have challenged the ability of journalists to make such a judgement without the full, classified background to intelligence operations. While GCHQ eventually agreed to have off-the-record discussions with reporters to indicate what details were extremely sensitive and might cause harm, they were unable to either confirm or deny the content of any story. This in theory presented

Box 1: The Snowden Disclosures

Many of the principal allegations that have emerged from the Snowden disclosures concern the ability of intelligence agencies to collect and analyse Internet and international communications data in bulk. Other allegations relate to the intelligence-sharing practices between agencies in different countries, relationships between governments and communications service providers, and methods for computer network exploitation (hacking). With the exception of PRISM, a US programme avowed by the US government, the information contained in the documents published has neither been confirmed nor denied by the UK government.

A number of the disclosures relate to the ability of the NSA and GCHQ to collect large volumes of data. For example:

- PRISM was said to involve the collection by the NSA of various data (including e-mail, photo, video and social-networking details) from the servers of nine US Internet companies (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple)
- The UPSTREAM programme was said to involve the collection by the NSA of communications from fibre-optic cables and other infrastructure carrying Internet traffic, rather than from the servers of Internet companies
- The TEMPORA programme related to GCHQ's ability to intercept digital traffic flowing through submarine fibre-optic cables landing in the UK
- The MUSCULAR programme was said to be a joint NSA–GCHQ programme which intercepted internal fibre-optic cables used by Google and Yahoo to transmit unencrypted data between their data centres
- Under the FASCIA programme, the NSA was said to track the movements of mobile phones by collecting location data
- Developed by the NSA, the XKEYSCORE system was said to allow analysts to carry out a search, using a search term such as an e-mail address or telephone number, across three days' worth of unfiltered data collected via a number of programmes such as PRISM and UPSTREAM.

Source: Anderson Report*, Annex 7*

8. Evidence to the ISR Panel, March 2014.

the problem of not being able to deny an untrue or incorrect story. Representatives from *The Guardian* noted that conversations with GCHQ were, however, more constructive than with US agencies.

3.12 The public's reaction in the UK to the Snowden disclosures has been markedly different than in the US (though there are some similarities). Representatives from *The Guardian* told us it was difficult for them to start a political and legal debate in the UK because they were marginalised by other media outlets as a result of the Leveson Inquiry into phone-hacking and media ethics. In addition, there are significant differences between the NSA and GCHQ, including the nature of their domestic operations, the legal frameworks governing them, and thus the nature of the allegations made against them.

3.13 Reactions to the Snowden disclosures have been varied. Public opinion around the world has reflected degrees of dismay or suspicion towards the revelations, particularly of bulk data capture on such a scale.[9] In the US and the UK, government and intelligence-community sources have consistently maintained that the revelations have damaged national security: terror suspects have made efforts to re-route or conceal their communications from US-based CSPs, terrorist websites offer advice on what can be learnt from the disclosures, and police services report a degradation of their ability to trace criminals.[10]

3.14 The disclosures accelerated a number of existing trends, such as the increased use of sophisticated, end-to-end encryption techniques and declining co-operation from CSPs. Intelligence officials and anonymous intelligence sources in the media have also said, however, that the Snowden disclosures have had specific consequences for UK national security. In particular:

- The police and GCHQ's ability to track domestic and foreign criminal gangs – including those relating to people trafficking and drugs – has been reduced[11]
- A video released onto a jihadist platform outlined what they had learned from the Snowden disclosures, providing advice on how to avoid detection and listing software packages that protect against surveillance[12]

9. See Pew Research Center, 'Global Opposition to U.S. Surveillance and Drones, but Limited Harm to America's Image', Global Attitudes and Trends, 14 July 2014.
10. Richard Kerbaj, 'Snowden's Leaks Scupper Surveillance of Crime Gangs', *Sunday Times,* 8 June 2014; Robert Verkaik, 'Al Qaeda's YouTube Guide for Jihadists: Security Chiefs Spooked over Terror Video That Proves Extremists Are Using Leaks from US Spy Edward Snowden to Evade Justice', *Daily Mail*, 20 January 2015; Intelligence and Security Committee, uncorrected transcript of evidence, John Sawers, Sir Iain Lobban and Andrew Parker, 7 November 2013.
11. Sunday Times, 'Snowden's Leaks Scupper Surveillance of Crime Gangs', 8 June 2014.
12. Daily Mail, 'Al Qaeda's YouTube Guide for Jihadists: Security Chiefs Spooked over Terror Video that Proves Extremists are Using Leaks from US Spy Edward Snowden to Evade Justice', 20 January 2015.

- Foreign terror suspects realised that their communications potentially passed through the US (even if the individuals themselves were not based there) and learnt which CSPs were allowing the NSA to access these communications.[13]

The Security and Intelligence Agencies

3.15 The British government's national security policies aim to protect UK and British territories, nationals and property from a range of threats, including terrorism and espionage; protect and promote the UK's defence and foreign-policy interests; protect and promote the UK's economic well-being; and support the prevention and detection of serious crime.[14] The National Security Strategy sets out the whole-of-government approach to national security, which notes that it is not just the responsibility of the SIAs, but of all government departments and agencies: 'We will use all the instruments of national powers to prevent conflict and avert threats beyond our shores: our Embassies and High Commissions worldwide, our international development programme, our intelligence services, our defence diplomacy and our cultural assets'.[15]

3.16 The majority of intelligence – up to 95 per cent – gathered by the intelligence agencies originates from open sources. Intelligence from secret sources is used to support national-security aspects of government policy by providing information on relevant activities and developments which are secret or undisclosed and which could not be adequately monitored using regular or open sources. Because secret intelligence is difficult and expensive to collect it therefore requires a high degree of prioritisation.[16] The SIAs must ensure that their limited resources focus on what cannot be gathered from open or normal diplomatic sources.[17]

Intelligence Tasking

3.17 The intelligence and security agencies do not set their own priorities. The National Security Council (NSC) and the Joint Intelligence Committee (JIC) are responsible for tasking the SIAs in accordance with agreed requirements and priorities, funding and performance monitoring. And as with any public agency, the scope of the work of the SIAs remains subject to financial constraints. The Single Intelligence Account (the budget for the three agencies) is decided by ministers through the spending review process and audited by the National Audit Office (NAO). The budget for 2014/15 was £1.9 billion, with a real-terms increase to £2 billion in 2015/16.

13. John Sawers, Iain Lobban and Andrew Parker, uncorrected submission of evidence to the ISC Privacy and Security Inquiry, Public Evidence Session, 7 November 2013.
14. See Part One in HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (London: The Stationery Office, 2010).
15. *Ibid.*
16. ISR Panel visit to the FCO, March 2015.
17. ISR Panel visit to the FCO, March 2015, and SIS, May 2015.

3.18 The NSC process for Priorities for Intelligence Collection (PICs) sets out the priorities of SIS and GCHQ. The PICs are divided geographically and thematically and are set with a three-year outlook. They are reviewed annually. The intelligence agencies can also be set mid-year requirements in the form of a Temporary Intelligence Watch, ordered by the chairman of the JIC, in response to events unforeseen by existing PICs (such as the Ukraine crisis, Arab Spring or the emergence of ISIL). This ensures the process can be flexible when necessary. The PICs are informed by statements of demand from government departments, and take the form of detailed questions that align with specific policy objectives. They do not dictate what specific resources should be allocated; however, the intelligence agencies use the PICs to prioritise and guide their own resourcing decisions.

3.19 There have been some changes to the central-government machinery on national-security matters over the past five years. In January 2011, the prime minister and the Cabinet secretary asked the national security adviser and the chairman of the JIC to review how the central national-security and intelligence machinery and structures could best support the NSC. The key recommendation from the review was that the NSC's priorities should be the lead driver of the JIC agenda, following as closely as possible the NSC's agenda and timetable. The NSC meeting of senior officials was considered best placed to oversee the tasking of the JIC, in line with its core role of setting strategic direction for the NSC.

Functions of the Security and Intelligence Agencies

GCHQ

3.20 Gathering intelligence from communications is the core of GCHQ's activities. However, GCHQ's intelligence mission is not self-driven; its intelligence requirements and priorities are set by government ministers and all of GCHQ's activity has ministerial endorsement. The organisation believes it is right that only ministers should make such decisions, judging intelligence priorities based on the likelihood of threats on the National Risk Register. GCHQ's activity includes counter-terrorism, cyber and military support (10 per cent of GCHQ's work force are serving members of the armed forces). 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.

3.21 GCHQ are also the government's lead agency on cyber-security and information assurance. In this regard, GCHQ therefore works very closely with government to ensure future data security, and its technology specialists frequently advise industry, law enforcement and government on cyber-security. Examples of this assistance include help with the rolling out of the Universal Credit benefit system (which will put payments equivalent to 8 per

cent of GDP online, representing a major potential vulnerability); the introduction of the replacement to the Airwave emergency communication network; and specific threats, such as the Gameover ZeuS malware used for banking fraud.

3.22 GCHQ also lead on supporting military operations of all types, with some military assets operating under GCHQ strategic direction. It supplements military signals-intelligence capabilities and its assistance has ranged from long-term analysis in the development of weapon systems and assessments of future threats, through to tactical support in helping adapt countermeasures against hostile states and actors. GCHQ has offered extensive support to UK military actions in Afghanistan and Iraq.

3.23 GCHQ work closely with MI5 to support their highest-priority operations and has contributed to the majority of MI5's counter-terrorism operations. It focuses primarily on the foreign and upstream elements of these operations, and how UK threats interact with these elements. In this regard, it is closely involved with operations in Syria to tackle the threat posed by ISIL.

3.24 GCHQ's intelligence mission covers a spectrum from long-term operations to tactical support: GCHQ support the NCA to focus on the 'top' organised-crime groups and activities, which include people and commodity smuggling. It has directly contributed to drug seizures. It also supports the NCA's Child Exploitation and Online Protection Command.

3.25 Data interception is fundamental to the work of GCHQ and forms an essential part of its tradecraft. Whereas in the past it was relatively straightforward to intercept telephone data, the job of data interception is now much more complex. Analysts must now both identify the target and work out by what means they are communicating, before they can begin to consider intercepting the content of their messages. Targets also use multiple and constantly changing personas, representing a major and continual challenge.

3.26 Only by filtering large volumes of information do GCHQ staff believe they can identify, and analyse data on, a selected target. Collecting this data in bulk is potentially problematic, from a privacy perspective, because of the sheer number of individuals whose communications are affected. Even if an individual's communications are never actually read – for example, an electronic communication which was obtained pursuant to a bulk data collection exercise but not selected for scrutiny – the fact that it *could* be read is regarded by some as placing control in the hands of the state.[18]

3.27 Officials were keen to stress that GCHQ employees are aware they are the guardians of what is potentially a very intrusive set of capabilities to collect this data. From their perspective, the greater risk of intruding upon an individual's privacy occurs at the point at which the data is analysed, rather than collected. As the information is filtered, more and more specific filters are applied before analysts can select any communications

18. David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* [Anderson Report] (London: The Stationery Office, 2015), p. 26.

to examine or read. According to the ISC, 'This involves complex searches to draw out communications most likely to be of greatest intelligence value and which relate to GCHQ's statutory functions. These searches generate an index. Only items contained in this index can potentially be examined – all other items cannot be searched for, examined or read'.[19]

3.28 At each stage, a judgement on necessity and proportionality is made. These judgements are made not only for ethical and legal reasons, but also practical reasons, in order to quickly focus on the most serious threats. In this way, good legal compliance and good business practice become one and the same; as noted by the ISC, GCHQ only has the capacity to analyse a fraction of available information, so the goal is both to be minimally intrusive and to maximise returns, filtering data to generate the smallest number of high-quality leads.

MI5

3.29 MI5 are a security and intelligence organisation. It is charged to act in the interests of national security; for the purposes of preventing or detecting serious crime; and safeguarding the economic well-being of the UK. While working under the objectives set by the NSC, MI5 are tasked slightly differently, and is set more generic priorities by government compared to its sister agencies. Around 65 per cent of MI5's effort and resources are dedicated to countering terrorism, while 10 per cent of the agency's work involves working with the Centre for the Protection of National Infrastructure (CPNI) in securing physical, personnel and cyber-security in the UK. Unlike SIS and GCHQ, MI5 is tasked to carry out national security investigations in addition to gathering intelligence.

3.30 MI5 possess significant technological capabilities, though it will seek the expertise of GCHQ where necessary. MI5's relationship with GCHQ has changed significantly over the last five years, particularly given the more extensive role of Internet communications. It is able to utilise GCHQ's capabilities (and vice versa) with Home Office agreement.

SIS

3.31 SIS collect secret intelligence and mounts covert operations overseas in support of British government objectives. The Panel were told that the use of intercept material, communications data and bulk data sets is crucial to its activities. Technology has had a fundamental impact on all aspects of the work of SIS: in identifying new agents, communicating with agents, understanding the operational environment and understanding the capabilities of hostile actors.

3.32 SIS needs to maintain a net technological advantage over adversaries; it recognises the responsibilities that this confers, and the accountability and oversight mechanisms that

19. Intelligence and Security Committee of Parliament (ISC), *Privacy and Security: A Modern and Transparent Legal Framework* (London: The Stationery Office, 2015), p. 112.

are required. It seeks to work with government and industry partners abroad, but many of these relationships have recently deteriorated. A concern highlighted by SIS was that if it cannot operate effectively online then it risks becoming irrelevant. In early 2014, it created a dedicated data directorate, recognising data as a transformational priority for the organisation and the significant opportunities and challenges it presents.

3.33 SIS's operations are split into seven regional networks and a number of SIS stations. Operations are structured in missions, with the overseas network of stations delivering these missions and operations. Examples of SIS intelligence operations might be in seeking to acquire information on regime stability, state–neighbour relations, political opposition, military capabilities or a state's attitudes towards the UK. Operations involve maintaining liaison relationships with foreign partners. SIS stations overseas are increasingly becoming 'SIA stations' as they house staff from across the three British intelligence and security agencies – particularly as MI5 now has the responsibility to investigate threats to the UK from overseas. It also allows agencies undertake joint operations more frequently.

The Use of Intrusive Capabilities

3.34 The SIAs have a range of different techniques and capabilities that they can exploit in order to gather intelligence and identify and investigate threats to national security. Much of the time these will not intrude upon the lives of British citizens – such as analysing open-source information and consulting public records.

3.35 At the same time, the SIAs are granted significant powers, with the appropriate authority, to employ more intrusive techniques to fulfil their mission. The degree to which they are intrusive differs as a result of factors including whether they operate in a public, private or electronic space, whether they involve deception, and whether they are targeted or untargeted. These techniques include:[20]

- Directed surveillance: observing someone covertly in a public place to gain private information about them
- Intrusive surveillance: covert surveillance carried out within a building or private vehicle. Typically, this involves attaching or embedding a recording device to monitor the activities of an individual
- Covert human intelligence sources (CHIS): the use of agents, undercover officers or informants to collect intelligence
- Camera surveillance: CCTV cameras, automatic number plate recognition and cameras on private property and widely used by authorities for public safety
- Interception: a wiretap on a telephone line or the gathering of e-mails or text messages in the course of transmission, in order to gather both content data and communications data

20. Anderson Report, pp. 141–45.

- Access to communications data retained by CSPs: traffic data, service-use information and subscriber information, often obtained retrospectively from the provider.

3.36 As illustrated by the debate over surveillance and privacy in the wake of the Snowden disclosures, one of the most contentious capabilities is the interception of, and access to, communications – whether those of an individual or in bulk. In order for a CSP to intercept the communications, they must be provided with a warrant signed by a secretary of state (typically the home secretary for warrant applications by MI5, and the foreign secretary for warrant applications by GCHQ and SIS). The legal framework for the warrant process is set out in more detail in Chapter IV.

3.37 Warrant applications must feature a Human Rights Act justification, in which the agency sets out what is commonly referred to as the triple test, designed to ensure that the warrant is:

- For a lawful purpose: the application must meet at least one of the three categories of intelligence requirement (in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the UK in circumstances relevant to the interests of national security)
- Necessary: the intrusion is needed to achieve one of the purposes listed above, and the information cannot be reasonably obtained by any other means
- Proportionate: the intrusion is reasonable in accordance with the intelligence requirement, and does not unnecessarily intrude upon the privacy of the individual (or those that might also be affected, such as the individual's family or close acquaintances).

3.38 Warrant applications go through a number of checks before they are finally approved. Internally within the relevant agency, the paperwork will be checked by warrantry staff and legal advisers before being submitted to a senior official, who will review the application and (if satisfied) sign it off on behalf of the head of the agency.

3.39 The application is sent to the dedicated warrant teams in the Home Office (in the case of MI5) and Foreign Office (in the case of SIS and GCHQ). Once again, the applications are checked and assessed, including ensuring that legal and policy advice is taken when needed, before being submitted to the secretary of state for their decision. At any point in this process, the application can be returned to the analyst for modification, clarification or additional information.

3.40 The current Home Secretary Theresa May has said that warrantry decisions occupy 'more of my time ... than anything else'. She dealt with the majority of over 2,700 warrants that were handled by the Home Office in 2014, personally authorising 2,345

interception and property warrants and renewals during that year.[21] And, as discussed in Chapter IV, warrant applications and approvals for the interception of communications and interference with property are periodically audited by senior judges, in the form of the commissioners.

3.41 A strong culture of dedication and compliance appears to exist across the three SIAs. Reports from the ISC and various commissioners acknowledge the culture of dedication to and compliance with internal policies within these agencies. Although the ISR Panel were unable to undertake an extensive assessment, given the timescales involved and the lack of powers to request access to information, the Panel did not encounter any evidence to suggest otherwise.

3.42 The ISR Panel were able to view GCHQ's Ethical Framework guidance for staff. While the content of the framework is not in the public domain, clear guidance is in place for employees who may have any ethical concerns over their work. We were told that ethical concerns can be raised and discussed freely, particularly with a dedicated ethics counsellor[22] who is available to staff and works in parallel to the staff counsellor, an external appointee who works across the three agencies and who 'is a point of contact for any members of the security and intelligence agencies who have anxieties relating to the work of their Service which it has not been possible to allay through the ordinary processes of management or staff relations'.[23] A whistle-blowing policy (which pre-dates the disclosures of Edward Snowden) provides a mechanism by which employees can raise any concerns over perceived malpractice or impropriety.

Key Challenges for the Security and Intelligence Agencies

3.43 This section draws out three key challenges to the operations of the SIAs, which became clear to the ISR Panel during their review; Chapter IV addresses the issues of legislation, oversight and accountability.

Keeping Pace with Technology

3.44 As detailed in Chapter I, the current pace of technological change continues unabated. An estimated $3 trillion is invested in the Internet globally each year and it is increasingly hard for governments to compete with the scale of private-sector investment. The number of Internet-connected devices continues to proliferate. The lack of sufficient technical understanding among policy-makers and many of the agents of government is part of a broader national deficiency that one of the ISR Panel members has already highlighted in a prominent forum. According to Martha Lane Fox, only one British organisation – the BBC – features among the top hundred most-visited websites in the world, ranked 74th, while some 10 million adults in the UK – half of them of working age – are not online and

21. *Ibid.*, p. 131.
22. MI5, SIS and GCHQ each have their own ethics counsellor.
23. SIS, 'Well-Being', <https://www.sis.gov.uk/careers/working-for-us/well-being.html>.

are disproportionately among the most disadvantaged socio-economic groups, whereas 90 per cent of new jobs require some digital skills. Only 30 per cent of UK small and medium enterprises currently buy or sell online, failing to reach a full potential which could be worth £18 billion to the national economy.[24]

3.45 The government wants Britain's digital society to reach its full social and economic potential. That will require a much greater willingness, at all levels, to learn and be educated in the digital technologies of our age. The evident need for greater technical literacy among the policy-makers and legislators who make decisions about surveillance and intrusion should be viewed on this wider canvas.

3.46 The SIAs are constantly developing their technological capabilities. However, they face challenges in retaining staff, with the private sector able to offer better pay and skills and career development. There is a need for active efforts to attract staff from the private sector back to the public sector.

3.47 The growth of the Internet and the digital economy has affected all levels of capability for the SIAs. Almost all investigations and operations now have an online aspect; everything an individual does online leaves a digital 'footprint', and the SIAs must be able to understand these traces of digital data. It would be strange in 2015 for an individual *not* to have a digital profile – and this will be almost impossible by 2020. Rather than provoking a fundamental shift in CSP and target behaviour, the disclosures by Edward Snowden have accelerated existing trends. For example, as targets are more security-aware, it has become much harder to intercept communications and to counter encryption (an issue discussed in further detail below). Of real concern is that co-operation from CSPs has reduced – a key issue for the police and NCA as well. This means that, like the police, the SIAs must now think more creatively and go to different, and more complicated, lengths to achieve their operational aims, which needs to be appropriately reflected in the governing legal framework.

Data

3.48 The volume of data in society has proliferated as a result of the increase in the number of services on the Internet; the proliferation of Internet-enabled device technology and increasing numbers of such devices; increased public use of cloud-based services; and public WiFi connectivity. Intelligence agencies are therefore now required to liaise with multiple service providers. However, while the number of Internet suppliers and stakeholders has increased, there has generally been a corresponding decrease in their co-operation with the police and the agencies. Those headquartered or with infrastructure abroad are less likely to recognise the extraterritorial reach of RIPA 2000, and therefore the validity of UK warrants within their jurisdiction. Evidence from some CSPs suggested that trust was an issue with SIAs, particularly in light of the Snowden disclosures.

24. Martha Lane Fox, speech delivered at the 2015 Richard Dimbleby Lecture.

3.49 Communications data is more important now than it has ever been for agencies with investigatory powers, but content is becoming increasingly difficult to access because of the growth in sophisticated encryption. Encryption reduces access to content, rather than access to communications data, by rendering it inaccessible without a key. When the service provider that holds the key is located within another jurisdiction, access becomes even harder.

3.50 The use by the agencies of bulk personal data sets (described earlier in Chapter II) was recently avowed by the ISC. These data sets are used primarily to validate and enhance existing intelligence. They may be data sets that only the government and its agencies have authorisation to access (such as electoral rolls, or the passport database). These data sets may not remain useful for very long and their utility is reviewed regularly; if there is no reasonable and legitimate reason for keeping the data set, it will be disposed of. These data sets are processed in the UK and are therefore subject to the DPA 1998 (though this contains exemptions for national-security purposes) and subject to statutory oversight by the Intelligence Services Commissioner.

Encryption

3.51 The issues and complications for intelligence and law enforcement surrounding encryption are clearly articulated in David Anderson's recent report and highlight the conflicting opinions of privacy advocates and security officials.[25]

3.52 As discussed in Chapter I, encryption is an integral part of Internet communications, and is necessary to ensure that, for example, online transactions remain secure. There are benefits and risks involved with end-to-end encryption (whereby the data can only be decrypted by the receiver and not by the CSP or any other intermediary). The degree to which data is encrypted has consequences for policing and national security, however.

3.53 In the private sector, CSPs have begun to introduce end-to-end encryption more extensively, particularly in the US market. This presents the police and SIAs with a significant challenge if they are looking to monitor the communications of individuals who pose a risk to collective security. They are increasingly concerned by the fact that many of the subjects of interest – including those in the highest-priority investigations – are able to use means of communication to which they no longer have access. It is this lack of detailed intelligence available on a small number of high-priority targets that is the prime concern, rather than broader intelligence available on a large number of low-priority targets. As noted by Anderson, the agencies 'struggle with the growth of encryption and the diversification of the communications market', and argue that 'if they cannot maintain their capabilities, threats will go undetected and opportunities to disrupt the ill-intentioned will not be identified'.[26]

25. See Chapter 4 (Technology) in Anderson Report, 4.44-4.71.
26. *Ibid.*, p. 195.

3.54 Anderson also points out, however, that law-enforcement and intelligence agencies do not have a technological edge over their adversaries, 'whether through crypto-analytical power, back-door access or partnership with other agencies'.[27] Equally, the agencies 'do not look to legislation to give themselves a permanent trump card: neither they nor anyone else has made a case to me for encryption to be placed under effective Government control, as in practice it was before the advent of public key encryption in the 1990s'.[28]

3.55 As we consider what powers of surveillance the SIAs have, there is a need for better understanding of the benefits and disadvantages of end-to-end encryption, as well as consensus on what data, if any, should be off-limits to authorities (and the consequences of this decision). As it stands, there seems to be broad public agreement that agencies such as the NCA and MI5 should be able to access data under legal and properly authorised circumstances. Encrypted data should not, as a principle, be beyond the reach of law enforcement; it is important that the relevant agencies are able to work with CSPs and seek to access information that will protect the public from (imminent) threats.

The Police and Law-Enforcement Agencies

3.56 There are forty-five territorial police forces in the UK, of which the Metropolitan Police is the largest. The NCA is a non-ministerial department set up in October 2013 to lead the UK's response to serious and organised crime. 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. The ISR Panel visited the NCA and Metropolitan Police, and met with representatives from the College of Policing and National Police Chiefs' Council.

3.57 A common theme from the ISR Panel's meetings, evidence sessions and research is that digital intelligence is central to police and law-enforcement response in the twenty-first century. According to the government, an estimated 95 per cent of serious and organised crime, domestic violence and cyber-crime investigations will use communications data. Evidence from the Metropolitan Police highlights that the majority of communications data is sought to manage risks to vulnerable members of society, victims of crime and the general public. Seventy per cent of urgent cases that the Metropolitan Police respond to relate to vulnerable people – for example, those at risk of suicide, those with mental health issues or potential victims of child sexual exploitation.

3.58 Given their often transnational nature, organised criminal groups make full use of modern communications technologies and data mining, and the Internet facilitates

27. *Ibid.*, p. 195.
28. *Ibid.*, p. 195.

'volume crime' in terms of new forms of fraud and theft. There are three issues specific to policing capabilities, all of which continue to pose a serious challenge:

- Diversification and technical change in electronic communications
- Communications are often held in multiple or foreign jurisdictions, requiring multilateral co-operation between states
- Criminals are early adaptors of digital technology and so are quick to exploit any blind spots, such as using Tor and virtual private networks.

3.59 The public expect the police and NCA to respond to all forms of criminality. To that end they need appropriate capabilities nationally, regionally and locally. However, 'traditional' forms of crime are no longer geographically focused; criminality has become digitally enabled and law enforcement cannot respond on a purely localised basis – a fundamental change to the British approach to policing. Online victims and offenders are often in different geographical locations, so it is often difficult to establish who has responsibility to look after the victim and ownership to investigate the suspect.

3.60 The number of criminal suspects may not necessarily have increased, but their communication through a variety of channels and platforms has grown. Whereby communications historically went through a single service provider, the situation today is much more complex and law-enforcement agencies must engage with, and request data from, an ever-growing number of CSPs, hardware and software providers, as well as applications available on smartphones and tablets.

Police Use of Communications Data

3.61 Communications data is used across a range of Metropolitan Police investigations: murder, rape, missing persons, domestic abuse and harassment, child sexual exploitation, serious acquisitive crime and fraud. For example:

- Tracing rape and murder suspects is an extremely high priority, especially due to the short life span of forensic evidence. A murder investigation may involve as many as 500 applications for communications data
- Around 50,000 people in London go missing each year. The Metropolitan Police pursues around five new investigations involving high-risk individuals each day. In the majority of cases, communications data is critical and there are many cases where an early arrest aided by communications data has prevented further harm. In extreme cases, for example where there is thought to be high likelihood of threat to life of a minor, hundreds of communications data requests can be made within a twenty-four-hour period
- DNA evidence is not always sufficient in many criminal investigations. Communications data can also be used to place suspects at the scene of a crime, as well as to prove that an individual was part of a conspiracy to commit an offence

- There has been a significant increase in the volume and sophistication of fraud offences. The National Fraud Intelligence Bureau make 16,520 referrals to the Metropolitan Police each year.

3.62 It is often difficult to know the ultimate value of information or data until the final outcome of an investigation, or to determine the value of communications data in securing a successful prosecution. There does not appear to be a common view among law-enforcement agencies on the most appropriate length of time for which data should be retained; and, indeed, it may vary per agency or type of data. It may also depend on the nature of the crime – financial-crime investigations, for example, can last months, if not years.

3.63 During the Panel's visit to the NCA, officers appeared satisfied with the current limit of twelve months for data retention. Any longer becomes unnecessary, as there are diminishing returns on data retained beyond this period; any shorter, however, would be problematic. Details from Operation *Notarise* – a substantial operation targeting people allegedly accessing child abuse images online – were used by the NCA to illustrate this. After 4,000 requests for communications data to trace who these individuals were, 92 per cent of suspects were identified, ultimately leading to 660 arrests. However, if the data retention period limit had been less than the current twelve-month period, the outcome would have been very different:[29]

- Only 13 per cent of suspects would have been identified had the data-retention period been three months
- Thirty-nine per cent would have been identified had the data-retention period been six months
- Sixty-six per cent would have been identified had the data-retention period been nine months.

Other Police Capabilities

3.64 There are several units within the Metropolitan Police which focus on specific aspects of digital policing, including the All Source Hub (ASH), Communications Exploitation Group (CEG), and Counter Terrorism Internal Referral Unit (CTIRU).

3.65 To respond to the growing use of social media, the Metropolitan Police created ASH in 2009. The creation of ASH was in response to the need for one platform to analyse both open-source and police databases. ASH is primarily concerned with threats from disorder and domestic extremism, though it also undertakes a considerable amount of work in support of counter-terrorism. ASH has had to respond to the evolving role of social media in high-profile events. The London Riots of August 2011 were the first 'social-media event' for the Metropolitan Police and demonstrated to police across the country the challenges of monitoring social media. In 2012, ahead of the London

29. ISR visit to the NCA, March 2015.

Olympics, some 2,565 intelligence reports were created, following analysis of 31 million items across 56,000 social-media platforms. Similarly, photographs and geotags posted by foreign fighters in Syria have been used extensively to identify their likely locations and travel routes, and to build material and evidence for investigations.

3.66 The CEG is concerned with lawful intercept, cyber-operations, and the attribution of communications data. Its cyber-operations are particularly focused on detecting hacking, for example on the City of London or by Islamist extremists.

3.67 Extremist groups continually search for new ways to circulate extremist or harmful material; websites justpost.it and archive.org are currently among the most popular. New internet companies and apps are also constantly emerging, posing challenges for investigators who often do not know from whom they should request data. Officers have also noticed that many of the new, and often smaller, internet companies are less comfortable with co-operating with law-enforcement agencies. Some are keen to ensure the online anonymity of their customers, and therefore do not retain data that could be passed to law enforcement; others are keen to first notify the customer that a law-enforcement agency has requested their data.

3.68 Lastly, there is a need sometimes for law enforcement to 'mix in with the noise' and covertly operate across multiple platforms when investigating crime and disorder. However, during such investigations they must be careful not to leave a digital footprint themselves; they do not want offenders to know that law-enforcement agencies are monitoring them.

3.69 The CTIRU was formed in February 2010 to seek out terrorist material online, as well as receive referrals from the public, partner agencies and colleagues elsewhere in the police. The CTIRU removes over 1,000 items a week from websites; most of the material is terrorist propaganda or instruction material (for example, on how to build explosives). This is an ongoing task and the unit recognises that it is impossible to ever have a clean Internet, free from such material.

3.70 In addition to the challenges facing the SIAs outlined above, the Metropolitan Police and other law-enforcement agencies identify the lack of co-operation from CSPs, particularly those based in foreign jurisdictions, as a significant ongoing challenge. There has been some progress and direct lines of contact have been sought and forged to ensure a priority service in urgent cases. Feedback has suggested that CSPs generally co-operate more readily with requests to remove material related to terrorism because they are high-impact, visible crimes and it is usually straightforward to demonstrate that the content does not conform to the CSP's terms and guidelines. However, the ISR Panel were told that the further an investigation moves away from counter-terrorism, or immediate 'threat-to-life' criminality, the harder it generally becomes to secure co-operation.

Other Government Agencies with Access to Communications Data and Surveillance Powers

3.71 Under Section 6(2) of RIPA 2000, an interception warrant can be issued in response to an application made by or on behalf of nine named office-holders.[30] Alongside more obvious individuals such as the director general of MI5 and the chief of Defence Intelligence (Ministry of Defence), they include the commissioners for the HMRC.[31]

3.72 A number of other public agencies have the power to access communications data, in support of the legal duties laid upon them which generally do not relate to security or policing (for example, environmental protection). The acquisition and use of this data is not well understood by large portions of society. The purposes for which public authorities may seek to acquire communications data are nevertheless restricted. Their ability to access each type of communications data (traffic data, service-use information and subscriber information) also depends on the authority in question.[32]

3.73 Several attention-grabbing headlines and media articles have brought these other agencies to greater public prominence, particularly when powers granted under RIPA 2000 are not used as expected.[33] For example, in 2008 Poole Borough Council admitted to using RIPA 2000 powers to monitor a mother's movements for nearly three weeks to find out if the family was telling the truth about living within a particular school catchment area. The local council used directed surveillance on six occasions under the auspices of the prevention or detection of crime, claiming that it was proportionate in determining whether the mother had been truthful. However, the activity was labelled as 'disproportionate' and 'intrusive' and the IPT subsequently found the Poole Borough Council guilty of improper use of surveillance powers and acting without justification.

3.74 The example illustrates the problematic nature of surveillance by government authorities. On the one hand, some believe it is perfectly reasonable for a council to conduct proper checks to ensure those qualifying for school places are entitled to do so (particularly in parts of the country where there is significant pressure on school places).[34] On the other hand, some believe that such surveillance – whether directed or via the interception of communications – is so intrusive that it should only be used in circumstances of national security, and not to allow for snooping by council officials.

30. In the context of a Mutual Legal Assistance Treaty the request may also come from 'a person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside the United Kingdom'.
31. See the Regulation of Investigatory Powers Act 2000 (RIPA 2000), 'Interception Warrants', Section 6(2).
32. Anthony May, *Report of the Interception of Communications Commissioner: March 2014* (London: The Stationery Office, 2015), p. 43.
33. Murray Wardrop, 'Councils Have Mounted Millions of Snooping Operations in Past Decade, Finds Report', *Daily Telegraph*, 4 November 2011.
34. Judith Burns, 'Schools Face "Places Breaking Point"', *BBC News*, 13 January 2015.

3.75 Privacy and civil-liberties groups have been vocal in their opposition to what they perceive as the use of intrusive powers by local authorities. A 2010 report by Big Brother Watch regarding the use of RIPA 2000 powers by local authorities highlighted a number of concerns, further fuelling the debate:[35]

- Councils alone have carried out over eleven surveillance operations every day over the past two years
- Over a dozen authorities have used RIPA 2000 powers to spy on dog owners to see whose animals were responsible for dog fouling
- Five authorities have used their powers to spy on people suspected of breaking the indoor smoking ban
- Suffolk County Council used RIPA 2000 powers to make a 'test purchase' of a puppy.[36]

3.76 Although RIPA 2000 clearly set out who the Act's main 'customers' or users are, the degree to which local authorities had access to the same intrusive powers as the SIAs has come as a surprise to some and caused significant concern for others. Some civil-liberties organisations are particularly critical of the perceived low threshold for authorisation necessary to invoke certain powers under RIPA 2000, and whether the use of its powers by some public sector bodies is truly proportionate to the circumstances:

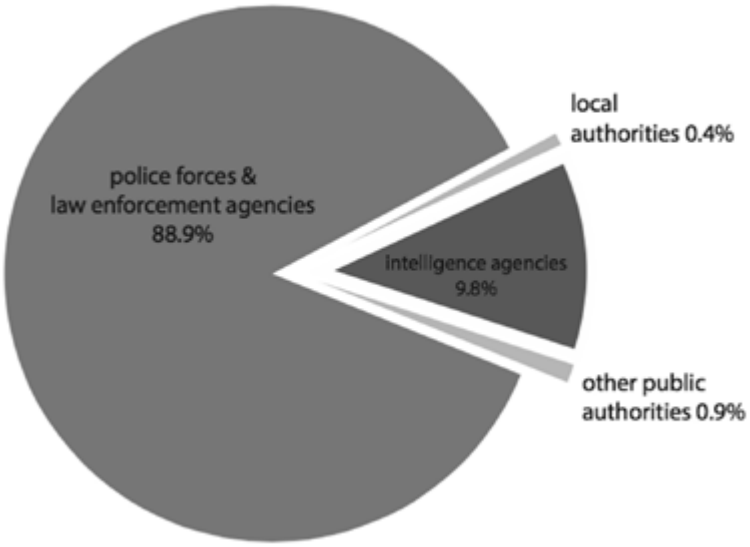
> [W]e must decide what sort of society we want to live in. It would reduce crime and disorder to ban alcohol or the motorcar or introduce a night curfew. We don't do these things because it would be disproportionate and illiberal. Equally, to many people, the possession of such intrusive powers by councils will seem unnecessary to the ends they seek to achieve. With very many of these things councils 'investigate' it may be concluded that the cure is much worse than the disease.[37]

3.77 In 2010, the new coalition government announced that it would 'ban the use of powers in the Regulation of Investigatory Powers Act by councils, unless they are signed off by a magistrate and required for stopping serious crime'.[38] In accordance with the Protection of Freedoms Act (which came into law in May 2012), the use of RIPA by local authorities now requires the approval of a magistrate and directed surveillance can only be used in cases whereby conviction would result in a custodial sentence of at least six months.[39] The Protection of Freedoms Act 'introduced a long overdue needed safeguard against unwarranted local authority surveillance', according to Big Brother Watch.[40]

35. The report was published before the then Coalition government met its commitments to curbing the abilities of Councils to use RIPA.
36. Big Brother Watch, 'The Grim RIPA: Cataloguing the Ways in Which Local Authorities Have Abused Their Covert Surveillance Powers', 2010, p. 1.
37. *Ibid*., p. 7.
38. HM Government, 'The Coalition: Our Programme for Government', 2010.
39. Duncan Gardham, 'Shake-up of Counter-Terrorism Laws Hits Councils', *Daily Telegraph*, 26 January 2011.
40. Big Brother Watch, 'A Legacy of Suspicion: How RIPA Has Been Used by Local Authorities and Public Bodies', 2012, p. 3.

3.78 In 2014, a total of 639 applications and 4,625 notices and authorisations were made by public authorities other than the SIAs and police and law-enforcement agencies, under Chapter II, Part I of RIPA 2000, excluding those given orally.[41] Figure 5 shows that the combined number of authorisations and notices by local authorities and other public authorities amounted to just 1.3 per cent of the total, although this was an increase on the 2013 figure (0.8 per cent).

Figure 5: Authorisations under Chapter II, Part I of RIPA 2000 and Notices by Type of Public Authority, 2014.[42]



3.79 Not all public-sector bodies have felt it necessary to regularly use powers granted under RIPA 2000. Of the 'other public authorities' granted powers under RIPA,[43] thirteen reported that they did not approve any applications, grant any authorisations or give any notices during 2014, the same number as in 2013. 172 local authorities reported

41. IOCCO 2014 caveat: the main report has highlighted the fact that the statistics IOCCO is currently able to collect under Paragraph 6.5 of the Communications Data Code of Practice are flawed and potentially misleading. There are essentially two difficulties with the authorisation and notice statistics: some public authorities may request multiple items of data on one authorisation or notice; and there are a number of different workflow systems in use by public authorities which have different counting mechanisms for authorisations and notices. It should also be noted that an application for communications data may contain a request for one item of data or many items of data, and some public authorities require applicants to submit different applications for different types of communications data. Because of the variability between applications and the inconsistent counting and aggregation of data requests on a single authorisation and notice, the statistics, although accurately recorded by each individual public authority, are not necessarily comparable.
42. May, *Report of the Interception of Communications Commissioner: March 2015*.
43. Prior to the removal of powers from those identified under SI 2014/228.

never using their powers to acquire communications data. Ninety-five local authorities reported using their powers in 2014, during which there were 319 total applications and 2,110 total notices and authorisations granted.[44]

3.80 On 12 February 2015, an amendment to the legislation resulted in thirteen public authorities with access to communications data under Chapter I of Part I of RIPA 2000 having their powers removed,[45] listed below along with the number of notices and authorisations (excluding urgent oral) granted in 2013 shown in brackets:[46]

- Royal Mail Group (119)
- Department for Business, Innovation and Skills (34)
- Environment Agency (18)
- Port of Liverpool Police (12)
- Civil Nuclear Constabulary (11)
- Department of the Environment (Northern Ireland) (1)
- Charity Commission (0)
- Department of Agriculture and Rural Development (Northern Ireland) (0)
- Department of Environment, Food and Rural Affairs (0)
- Food Standards Agency (0)
- Pensions Regulator (0)
- Port of Dover Police (0)
- Scottish Environment Protection Agency (0).

3.81 Powers were also granted to the Financial Conduct Authority and the Prudential Regulation Authority in order for them to be able to 'obtain communications data for the purpose of exercising functions relating to the regulation of financial services and markets or to financial stability'.[47]

3.82 The use of communications data by all agencies, including local authorities, is overseen by the Interception of Communications Commissioner. According to the IOCCO 2014 Annual Report:

> [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

44. May, *Report of the Interception of Communications Commissioner: March 2015*.
45. Home Office, 'The Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2015', SI 2015/228.
46. Anthony May, *2013 Annual Report of the Interception of Communications Commissioner* (London: The Stationery Office, 2014).
47. See explanatory note in Home Office, 'The Regulation of Investigatory Powers (Communications Data)(Amendment) Order 2015', SI 2015/228.

in the work that they carry out. There is a strong culture of compliance and of self-reporting when things go wrong.[48]

The Global Context

3.83 The challenges faced by the police and SIAs outlined in this chapter also have to be set in a wider context that recognises the much greater relevance of global industry and international politics to government interaction with the Internet. It requires a different frame of reference in considering domestic surveillance powers.

3.84 While Internet users once were predominantly from Western developed countries, this is no longer the case. Of the 40 per cent of the global population that currently has access to the Internet, Europe and North America account for less than half of this total. But future growth is much more likely to take place in South and East Asia, especially in India and China, in Africa and in Latin America. The US remains far and away the most important national actor in the politics and economics of the Internet, but the centrality of the US is diminishing as large CSPs develop in countries such as China, and the private sector disperses its operations across the globe.

3.85 Technical distinctions between communications that are domestic and that are international are now difficult to sustain. In the previous era of telephone landlines a national call was, by definition, a domestic communication. Now, internationally located servers mean that a communication between two people within the same country might, in reality, be via a foreign server and therefore be classed as international. What David Anderson calls the 'fragmentation of providers' continues to break down the technical distinctions between what is a domestic and an international communication, with all the attendant difficulties of attributing any particular communication to its original sender or recipient.[49] New challenges posed by cloud computing, for example, arise mainly from the storage of data outside the control of any single organisation in one legal jurisdiction, which is now less likely to be in the US or the UK. Such manifestations of extraterritoriality will undoubtedly become more acute as the number of users and internet companies based in Asia, Africa and Latin America increases.

National Jurisdictions

3.86 If the Internet, by its very nature, straddles all the national legal jurisdictions of its users, the fact remains that law-enforcement and intelligence organisations – as agents of the state – are by definition subject to jurisdictional boundaries.

3.87 The European Court of Human Rights provides binding instruments that govern certain aspects of the legal frameworks of its signatory members. This, however, does not cover non-European states and only some of the most relevant aspects of interception and

48. May, *Report of the Interception of Communications Commissioner: March 2015*, p. 2.
49. Anderson Report, pp. 52–54 (paras 4.17-4.25).

surveillance among its member states. Beyond that, a number of reviews have been conducted and guidelines suggested through the UN, the EU and the Council of Europe to suggest harmonisation measures that would bring law, practice and the culture of security closer together between states that are still catching up with the implications of Internet technology on their human rights as well as their security concerns.[50]

3.88 In addition, civil-society organisations in many Western countries have led a number of transnational initiatives suggesting more harmonised policy responses. Such initiatives have been said to constitute 'a growing array of international and European soft law on the oversight of security services' although there are 'relatively few binding, hard-law principles'.[51] Calls have been made for an 'international social compact' to guide the harmonisation of laws and practice within a multinational 'digital society' and the UN and the OECD, among other international organisations, have offered principles and resolutions that may help harmonise different laws, policies and cultures between countries prepared to co-operate.[52] So far, few of these calls have affected the jurisdictional complexity that Western governments face.

3.89 The legal challenges are evident. RIPA 2000 was intended to apply to CSPs operating within UK jurisdiction. The Data Retention and Investigatory Powers Act 2014 (DRIPA) provided explicitly that interception warrants could be served on any CSP operating within the UK, wherever their material was transmitted or stored. But it remains difficult for UK authorities to operationalise the international provisions of these pieces of legislation.

3.90 In its 2014 report on the terrorist murder of Fusilier Lee Rigby, the ISC expressed the problem forcefully saying that, 'none of the major US Communication Service Providers ... regard themselves as compelled to comply with UK warrants obtained under the RIPA'. DRIPA, they said, 'has represented some progress' but had not solved the problem for the UK, which 'is acute'.[53] They added that, 'In some circumstances, overseas CSPs may choose to comply with a request … even though they do not consider themselves bound by UK legislation'.[54] This was welcome but not regarded by the ISC as an adequate solution.

3.91 Jurisdictional issues are in many cases handled by governments through mutual legal assistance treaties (MLATs) in which requests for bilateral or multilateral assistance between partners are handled through established processes. In the current climate, the

50. Council of Europe, Commissioner for Human Rights, 'Democratic and Effective Oversight of National Security Services', Issue Paper, Council of Europe, 2015.
51. *Ibid.,* p. 33. Such governmental and private initiatives have found expression in the work of UN special rapporteurs on human rights and counter-terrorism; the Council of Europe's Venice Commission; the European Parliament's LIBE Committee; the 'Ottawa Principles' of 2006 or the 'Tshwane Principles' of 2013.
52. Global Commission on Internet Governance, 'Towards a Social Compact for Digital Privacy and Security', CIGI/Chatham House, 2015.
53. ISC, *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby* (London: Stationery Office, 2014), p. 7.
54. *Ibid.* p. 133.

US–UK MLAT is particularly relevant to the counter-terrorist policies of both countries. There is widespread agreement, however, that the process is normally too slow and cumbersome to meet the current levels of demand for speedy legal co-operation between partner countries. Even assuming a case in which there is complete agreement between officials in Britain and the US about the necessity to co-operate quickly to obtain national data, each country's need to follow its own due legal process could impose long delays – over a matter of months – to cases that may require speed measured in days or even hours. To date, there seems little likelihood that the mutual legal assistance treaty process will be substantially streamlined, since the legal requirements and traditions of partner countries are usually long-established and necessarily important to the country concerned.

Internet and Communications Service Providers

3.92 Like any major company operating internationally, the business models of internet companies and CSPs require them to be compliant in legal jurisdictions wherever they want to exploit a market. Major companies and CSPs increasingly move their servers – and services – into different states as they navigate to best commercial advantage around the jurisdictional complexity of their world.

3.93 In the matter of legal interception and co-operation with law-enforcement agencies, companies argue that they must contend with inconsistent jurisdictions in different countries, and also are caught between conflicting demands between governments wanting access to their data on the one hand and recent customer resistance to such access, which the Snowden disclosures have intensified, on the other.

3.94 Internet companies argued to the ISR Panel that they are nevertheless very conscious of their corporate social responsibilities, especially in matters of terrorism and serious crime. They point out that they respond very quickly to urgent requests from law-enforcement agencies where there is threat to life or an imminent terrorist attack might be at stake. They also point out that they often exercise careful judgement and restrict material on their sites which may not be illegal, but is simply contrary to company policy. On the other hand, they make a strong case that they are not qualified to be intelligence agencies, or make subtle judgement over what data and material might be regarded as connected to terrorism, espionage or organised crime. They obey the law in countries in which they operate but should not be assumed to be natural partners of any government in national security.[55]

Security and Intelligence Agencies across the World

3.95 Intelligence agencies, even those within the Western world, are not a homogeneous group with entirely similar interests. Differences of approach to interception also reflect their own national circumstances, and their interest in particular methods to intercept

55. Evidence taken by the ISR.

communications has largely stemmed from their own available access. As one analysis puts it: 'For the United States, it appears from recent disclosures that access to digital data via the dominant US Internet companies has been especially important; for the United Kingdom and France, for historical and geographical reasons, submarine-cable access has featured; for Germany, satellite access; for China and Russia, digital computer network exploitation appears from the cyber-security press to have been highly productive in recent years'.[56] In smaller countries, intelligence agencies frequently try to gain access to local commercial mobile networks, or simply rely on access to social media to monitor groups or public trends.

3.96 Even the biggest and most capable of intelligence agencies, therefore, rely on close co-operation with other intelligence services in like-minded countries alongside partnerships of varying intensity with a range of other foreign countries. For the UK, the Five Eyes intelligence relationship between the UK, US, Canada, Australia and New Zealand has been particularly important. Between the access the US previously had through US Internet companies and UK access to submarine-cable traffic, the potential of their joint monitoring capabilities has undoubtedly been high.

International Politics

3.97 The global nature of the Internet represents a new domain of international competition between traditional states. The adversaries of Western democracies have observed for themselves the potential power of Internet-based technologies. There is extensive evidence that some autocracies use their own state resources to stifle domestic dissent and pursue dissenters by localising, as far as they can, Internet access. There have been demonstrable efforts in countries such as Russia, China, North Korea and more recently in Iran, not only to restrict the potential social impact of freely available information and communication, but to turn the technology into new instruments of state control.[57]

3.98 This has direct relevance to security in the democratic world. Autocratic regimes that operate blanket restrictions in their own societies are able to exploit the vulnerabilities of a society heavily dependent on digital technology for many traditional adversarial purposes: intelligence, subversion, industrial espionage, economic disruption and so on. The cyber-attack on Estonia in 2007, widely believed to have originated from Russia, was a clear attempt to create economic harm and damage the Estonian government. The cyber-attack on Sony Pictures in 2014, widely attributed to North Korea, was apparently an attempt to retaliate against what was perceived as a national insult. Some autocratic

56. David Omand, 'Understanding Digital Intelligence and the Norms That Might Govern It', Global Commission on Internet Governance Paper Series, No. 8, CIGI/Chatham House, p. 8.
57. Rosemary d'Amour, 'Authoritarian Regimes and Internet Censorship', Center for International Media Assistance, <http://www.cima.ned.org/authoritarian-regimes-internet-censorship/>; Robert Orttung and Christopher Walker, 'Authoritarian Regimes Retool Their Media-Control Strategy', *Washington Post*, 10 January 2014; Shanthi Kalathil and Taylor C Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule* (Washington, DC: Carnegie Endowment for International Peace, 2003).

governments are suspected of assisting criminal groups in operating fraud and extortion rackets against democratic countries, on the basis that such operations are economically damaging and difficult to ascribe to any foreign government.[58]

3.99 Whilst maintaining all the restrictions appropriate to a democratic society in the interception and use of data for law enforcement and national security, Western governments nevertheless have to reckon with international adversaries that do not observe such restraints and whose policies can exploit more fully this new domain of international relations.

58. See National Security Council, 'Transnational Organized Crime: A Growing Threat to National and International Security', <www.whitehouse.gov/administration/eop/nsc/transnational-crime/threat>, pp. 3–4.

IV. Legislation, Oversight and Accountability

4.1 Public confidence in the acquisition and retention of data rests on the credibility and practicality of the legal and oversight frameworks that govern it. In respect to the government's use of surveillance powers, these have developed in an ad hoc manner as technology has advanced and there is growing consensus that the present legislation and oversight regime will not be adequate for the future. In the view of one observer, 'The agencies will work within the law, but the law has to be relevant to the digital age and has to be enforceable. Only then can the security services provide a comprehensible narrative to the public and Parliament such that there is a shared understanding of why enforcement is necessary. This narrative is essential and overdue'.[1]

4.2 The legal framework governing surveillance, the interception of communications and the use of data in the UK is notoriously complex. It is made up of different and overlapping pieces of domestic primary and secondary legislation, European directives and international conventions. The framework covers much of the remits of the law-enforcement agencies and SIAs. The principal parts of this framework are detailed below.

The Security Service Act 1989

4.3 The Security Service Act (SSA) 1989 placed MI5 on a statutory footing, under the authority of the secretary of state and under the control of a director general. The Act outlined the primary functions of MI5, namely:

- To protect national security 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
- To safeguard the economic well-being of the UK against threats posed by the actions or intentions of persons outside the British Isles
- To act in support of the activities of police forces and other law-enforcement agencies in the prevention and detection of serious crime.

4.4 The SSA 1989 introduced the principle of MI5 requiring a warrant to undertake certain activities, such as entry on or interference with property, which is unlawful unless 'authorised by a warrant issued by the Secretary of State'.[2]

1. Martin Moore, 'RIP RIPA? Snowden, Surveillance, and the Inadequacies of Our Existing Legal Framework', *Political Quarterly* (Vol. 85, No. 2, April/June 2014), p. 127.
2. See the Security Service Act 1989, s 3(1).

4.5 The Act also laid the groundwork for what would become the oversight commissioners, appointing a 'person who holds or has held high judicial office' to oversee the service, as well as the Investigatory Powers Tribunal (IPT), establishing a tribunal 'for the purpose of investigating complaints about the Service'.

The Intelligence Services Act 1994

4.6 The intelligence agencies were not avowed by the UK government until the passing of the Intelligence Services Act (ISA) 1994, which for the first time acknowledged in law the existence of both SIS and GCHQ. The Act outlined the role of SIS to 'obtain and provide information relating to the actions or intentions of persons outside the British Islands; and to perform other tasks relating to the actions or intentions of such persons'; the primary role of GCHQ, meanwhile, was to 'monitor or interfere with electromagnetic, acoustic and other emissions … to obtain and provide information derived from or related to such emissions or equipment and from encrypted material'. These functions were to be carried out in relation to issues of national security, economic well-being and to prevent and detect serious crime.

4.7 As with the SSA 1989, the ISA 1994 made provision for the issue of warrants and authorisations enabling certain actions to be taken by the intelligence agencies in relation to interference with property (broadly defined) and wireless telegraphy, noting that 'no entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State'. Under Section 5 of ISA 1994, SIS and GCHQ may therefore obtain authorisation to carry out equipment interference, including computer-network exploitation (CNE), in pursuit of their statutory functions and in specific circumstances. CNE was avowed for the first time by the government in February 2015 when it published the draft Equipment Interference Code of Practice, which made clear that equipment may include 'computers, servers, routers, laptops, mobile phones and other devices'.[3]

4.8 The ISA 1994 introduced the role of the Intelligence Services Commissioner (to review the workings of the two intelligence agencies in addition to the security service) and the IPT (to deal with complaints). It also established a system of Parliamentary accountability in the form of the Intelligence and Security Committee, in order to examine the expenditure, administration and policy of the three SIAs.

The Human Rights Act 1998

4.9 The Human Rights Act (HRA) 1998 was introduced in order to incorporate into UK law the fundamental rights and freedoms contained in the ECHR. Its effect is that all bodies carrying out public functions – from local authorities to the police and intelligence agencies (as well as the bodies that oversee them) – must not interfere with the

3. David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* [Anderson Report] (London: The Stationery Office, 2015), p. 101.

individual rights set out in the ECHR, and must ensure that their decisions are compliant with human-rights legislation.

4.10 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 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.

4.11 Among other things, it also means that individuals can take human-rights cases to domestic courts rather than having to take their case to the ECtHR.

The Data Protection Act 1998

4.12 The DPA 1998 confers on individuals certain rights, including the right to know what information is held about them; it also placed obligations on persons, organisation, businesses and the government to manage the personal information they hold in an appropriate way. These data controllers must comply with eight 'data protection principles', ensuring information is:[4]

- 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.

4.13 A new role in the form of the Information Commissioner was created by the DPA 1998 in order to oversee compliance with the Act.

4.14 The DPA 1998 covers personal data held on computer and in manual files, and also imposes restrictions on the transfer of data outside the European Economic Area, which has particular implications for placing material on the Internet. The DPA 1998 provides stronger legal protection for more sensitive information, such as ethnic background, political opinions, religious beliefs, health, sexual health and criminal records.

4. Gov.uk, 'Data Protection', <https://www.gov.uk/data-protection/the-data-protection-act>.

4.15 The DPA 1998 does not provide an absolute right to data privacy, but it does introduce a number of important safeguards to ensure data is appropriately handled by organisations. An exemption from the full requirements of the DPA 1998 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 Regulation of Investigatory Powers Act 2000

4.16 The ability of public-sector organisations to intercept communications has been on a statutory footing since the Interception of Communications Act 1985. However, this Act primarily concerned communications sent by post or fixed-line public-telecommunication systems, and the rapid changes in telecommunications in subsequent years, coupled with decisions by the European Court of Human Rights, prompted a government consultation in 1999. RIPA 2000 was enacted the following year, providing a legal basis for the lawful interception of communications and access to communications data, surveillance and the use of undercover agents and informers (also known as CHIS), and access to protected data.

4.17 There was also a need to establish new legislation in light of the requirements of the HRA 1998 and, in particular, the interference with an individual's right to privacy through intercepting the content of their communications. RIPA 2000 sets out the possible justifications for such interception, namely: in the interests of national security; for the purpose of preventing or detecting serious crime; for the purpose of safeguarding the economic well-being of the UK in circumstances relating to national security (as amended).[5]

4.18 One of the fundamental principles guiding RIPA 2000 is that a distinction can be made between communications data and content, with acquisition of the former considered less intrusive to an individual's privacy than the latter. Authorisations for the acquisition and disclosure of communications data are therefore issued by designated persons within the organisation seeking the data. However, in order to gain access to the actual content of a communication (for example, the text of an e-mail message or a telephone conversation), a warrant issued by the secretary of state is generally required.[6]

4.19 A second principle of RIPA 2000 is that there is a difference between 'internal communications' (that are both sent and received in the British Isles) and 'external communications' (in which the sender and/or recipient are outside the British Isles). There are therefore two types of interception warrant for which the individuals listed

5. Philip Ward and Alexander Horne, 'Interception of Communications', House of Commons Note, SN/HA/6332, 2015, p. 3.
6. *Ibid.*, p. 1. Under the Police and Criminal Evidence Act, content can also be requested via a judicial warrant.

above can make a submission. A warrant granted under Section 8(1) of RIPA (also known as an '8(1) warrant') must name or describe the subject of the interception, as well as the 'selectors' (such as an e-mail address, postal address, telephone number and so on) that will be used to identify the communications that are to be intercepted.

4.20 A warrant granted under Section 8(4) of RIPA (an '8(4) warrant') does not need to name the subject of interception, nor does it impose an express limit on the number of external communications which may be intercepted. This is the basis on which intelligence agencies are able to collect data in 'bulk'. If the requirements under this section are met, then the interception of all communications transmitted on a particular route or cable, or carried by a particular CSP, could, in principle, be lawfully authorised. According to the Home Office, 'This reflects the fact that section 8(4) interception is an intelligence gathering capability, whereas section 8(1) interception is primarily an investigative tool that is used once a particular subject for interception has been identified'.[7]

4.21 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 over 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'.[8]

4.22 Once a warrant has been issued, the intercepting agency is then authorised to carry out the interception or to call on the assistance of the relevant CSP, which is under a 'duty to take all such steps for giving effect to the warrant'.[9] Interception warrants issued on serious-crime grounds are valid for an initial period of three months. Interception warrants issued on the grounds of national security or economic well-being of the UK are valid for an initial period of six months, subject to renewal.

4.23 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).

4.24 A final important aspect of the RIPA 2000 legislation is that it put into statute the IPT, as well as the roles of the Interception of Communications Commissioner, the Surveillance

7. Home Office, 'Interception of Communications: Code of Practice', draft for public consultation, 2015, p. 19.
8. Home Office, *Interception of Communications: Code of Practice* (London: The Stationery Office, 2002), pp. 7–8.
9. RIPA 2000, Section 11(4).

Commissioner, and the Intelligence Services Commissioner. It also put into statute the establishment of Technical Advisory Board, designed to advise the home secretary on whether the obligations imposed on CSPs under the terms of the Act are reasonable.

4.25 RIPA 2000 has been subject to a number of criticisms. The subject of these criticisms typically falls into one of three categories:

- It is opaque and difficult to understand
- It has not kept up with the pace of technological change, particularly as the distinctions between content and communications data, and domestic and international communications, have become less clear
- The powers it grants have been abused by a small number of public-sector bodies.

4.26 Firstly, it has been criticised for being a particularly difficult piece of legislation to understand. JUSTICE, an independent law-reform and human-rights organisation, argued that 'it was not so much a comprehensive framework for surveillance powers so much as a crude stitching-together of different regulatory regimes that were each highly complex in their own right and, taken together, lacked all coherence'.[10] The legislation is accompanied, however, by periodically updated codes of practice.

4.27 Secondly, and as noted in Chapter I, the shape of the modern, digitised society has evolved rapidly since 2000, and continues to do so. Whilst RIPA 2000 was written with the stated intention of remaining technologically neutral, it was enacted just one year after Google published its first press release, and four years before Facebook was even conceived. Critics therefore argue that it is insufficiently specific in how the law applies to new Internet communications. One academic notes that RIPA 'was not written in the age of social media and big data. It is inherently backward-looking',[11] while the Reform Government Surveillance initiative highlights the fact that 'the law in this area simply has not kept pace with the scale of technological change ... gaps and weaknesses in the framework have been exploited to enable the collection of our private communications on a previously unimaginable scale'.[12]

4.28 RIPA 2000 took into account the fact that 'not all of the system parts were within UK territory, that devices and services could operate both within and outside of the UK and that services do not necessarily relate to a company based within the UK', and that it was intended to apply to CSPs 'offering services to UK users, wherever those companies and/or their telecommunication systems were based'.[13] However, it is acknowledged that this was largely implicit in the legislation, rather than explicit.

10. JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (London: Justice, 2011), p. 11.
11. Moore, 'RIP RIPA?', p. 127.
12. Don't Spy on Us, 'Don't Spy on Us: Reforming Surveillance in the UK', 2014, p. 10.
13. May, *Report of the Interception of Communications Commissioner: March 2015*, p. 15.

4.29 Thirdly, a final criticism relates to the application of powers under RIPA 2000, in terms of the number of organisations having access to these powers and the alleged abuse of these powers by certain public-sector bodies. Following allegations of the use of RIPA powers by the police to obtain journalistic material, and by local councils to 'spy' on citizens for perceived minor offences, the House of Commons Home Affairs Committee published a review of RIPA 2000 in December 2014 which concluded that it was 'not fit for purpose'.[14] Its main criticisms focused on the lack of information recording, and the level of secrecy surrounding the use of RIPA 2000, which 'allows investigating authorities to engage in acts which would be unacceptable in a democracy, with inadequate oversight'.[15]

European Directives and the *Digital Rights Ireland* Case

4.30 The RIPA legislation that provides government agencies with powers to intercept or acquire an individual's communications via a CSP is separate from the legal obligation of the latter to *retain* communications data for the purpose of investigation, detection and prosecution of serious crime and terrorism.

4.31 In the UK, under the Anti-Terrorism, Crime and Security Act 2001, telecommunications operators were asked to retain information on a *voluntary* basis with the understanding that they would be reimbursed for retaining and handing over data beyond their normal operations. A code of practice setting out the voluntary agreement was created through the Retention of Communications Data (Code of Practice) Order 2003.[16]

4.32 In the wake of the terrorist attacks in Madrid in 2004 and London in 2005, the EU adopted Directive 2006/24/EC, which imposed obligations on member states to adopt measures to ensure that communications data generated or processed by CSPs within their jurisdiction be retained for periods of between six months and two years (leaving it up to individual member states to decide their own retention periods within these limits).[17] The Directive was careful to note that CSPs were not being required to collect information that they did not already collect.[18]

4.33 This Directive was transposed into UK law by way of secondary legislation in 2009, the Data Retention (EC Directive) Regulations 2009 SI 2009/859. This made the retention of data by CSPs mandatory for twelve months (though CSPs may have their costs reimbursed). The regulations created the power for the home secretary to require CSPs, by notice, to retain communications data that they already held for business purposes for a period of twelve months.[19]

14. Home Affairs Committee, 'Regulation of Investigatory Powers Act 2000', Eighth Report of Session 2014–15, HC711, p. 11.
15. *Ibid.*, p. 11.
16. Ward and Horne, 'Interception of Communications', pp. 5–6.
17. *Ibid*., p. 5.
18. *Ibid.*, p. 6.
19. Liberty et al., 'Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN Briefing on the Fast-Track Data Retention and Investigatory Powers

4.34 In the *Digital Rights Ireland* case at the European Court of Justice (ECJ), the EU's 2005 Directive was challenged on the grounds of infringement of the right to private life, and the right to the protection of personal data of individuals, as guaranteed in Articles 7 and 8, respectively, of the Charter of Fundamental Rights of the European Union. The case was bought by the High Court in Ireland and the Constitutional Court in Austria, which asked the ECJ to examine the validity of the Directive, in particular in light of the Charter of Fundamental Rights. In April 2014, the ECJ declared the Directive invalid, declaring that 'by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data'.[20] The ECJ determined that the Directive represents a serious interference with these fundamental rights without limiting that interference to what is strictly necessary.[21] It also concluded that, in adopting the data-retention Directive, 'the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality'.

4.35 Given that the Directive was no longer valid, this meant that, to all intents and purposes, the secondary legislation introduced by the UK in 2009 was also invalid. A footnote to the Court's press release noted that this was with immediate effect, since 'the declaration of invalidity takes effect from the date on which the directive entered into force'.

The Data Retention and Investigatory Powers Act 2014

4.36 On 10 July 2014 the government announced that emergency legislation would be introduced on retention of communications data. The government stated that the need for the Bill was twofold. First, in light of the *Digital Rights Ireland* case, there was no legal basis for the government to ask CSPs to retain data for any length of time; it was therefore concerned that, unless they had a business reason to hold this data, internet and phone companies would start deleting it, fearing legal action.[22]

4.37 Secondly, the government sought to 'clarify' the extra-territorial reach of the RIPA 2000.[23] It amended the legislation to put beyond doubt that requests for interception and communications data made to overseas companies providing communications services within the UK are subject to the legislation. At the same time, the prime minister announced a series of other measures, including the establishment of a Privacy and Civil Liberties Oversight Board, half-yearly transparency reports on the use of

Bill', 2014, p. 4.

20. Court of Justice of the European Union, 'The Court of Justice Declares the Data Retention Directive to Be Invalid', press release, No. 54/14, 8 April 2014.
21. Liberty et al., 'Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN Briefing', pp. 7–8.
22. Ward and Horne, 'Interception of Communications', p. 2.
23. Liberty et al., 'Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN Briefing', p. 2.

surveillance powers and a further restriction on the number of public bodies able to request communications data.[24]

4.38 DRIPA 2014 had cross-party support and the Bill was fast-tracked through Parliament in less than seven days (a process that normally takes several months). This attracted criticisms from some MPs and civil-liberties groups, who claimed that there had been insufficient time to scrutinise and debate the implications of the legislation.

4.39 Critics also accused the government of trying to slyly re-introduce expanded capabilities contained in the Communications Data Bill which was previously blocked by Liberal Democrat opposition in 2012. This was, opponents argued, an attempt to expand the interception capabilities of the government in general and the SIAs in particular: 'In extending the territorial reach of the RIPA interception regime, the Government seeks to dramatically expand its ability to mandate the interception of communications content across the globe'.[25]

4.40 A group of fifteen technology-law academics wrote an open letter in which they claimed that DRIPA was 'far more than an administrative necessity; it is a serious expansion of the British surveillance state. We urge the British Government not to fast track this legislation and instead apply full and proper parliamentary scrutiny to ensure Parliamentarians are not mislead [*sic*] as to what powers this Bill truly contains'.[26] The government has committed to a review of the legislation governing surveillance by December 2016 when DRIPA expires; this ISR Report is intended to contribute to the debate leading up to this review.

The Oversight Regime

4.41 Robust and effective oversight and redress is 'an essential component in inspiring and maintaining public trust and confidence'.[27] As identified by the previous section, there are provisions within a number of pieces of legislation for scrutiny and oversight of the UK's intelligence, security and law-enforcement agencies. RIPA 2000 strengthened existing legislation under the ISA 1994 and the SSA 1989 to set out the legislative framework for the commissioners, Investigatory Powers Tribunal and the Codes of Practice.

4.42 Whilst greater oversight of intrusive activity is welcome, 'this proliferation of oversight mechanisms and regulators with, in some cases, overlapping responsibilities does means

24. Ward and Horne, 'Interception of Communications', p. 1.
25. Liberty et al., 'Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN Briefing', p. 3.
26. Jemima Kiss, 'Academics: UK "Drip" Data Law Changes Are "Serious Expansion of Surveillance"', *Guardian*, 15 July 2014.
27. Information Commissioner's Office submission to the ISR.

it is a complex framework that does not necessarily serve the public well as it is not always clear to individuals who they should raise their concerns with'.[28]

4.43 In a similar fashion to the legislative framework, the oversight framework has developed in a largely ad hoc manner. There must be clarity of oversight to secure and maintain enduring public confidence in the security, intelligence and law-enforcement agencies alike. In addition to the number and effectiveness of oversight mechanisms in place, any debate on the matter should therefore focus on the extent to which they are visible and credible in the eyes of the public.

Legal Oversight

4.44 Whereas in the past there was just one lawyer shared between the intelligence agencies, today there are substantial legal departments within each agency and employees can easily seek legal advice or clarification when required. Legal advice is available at every stage of the warrant and authorisation process for all public bodies authorised to conduct intrusive activity under RIPA.

4.45 Unlike much of the intelligence gained by the SIAs under Part I of RIPA 2000, evidence secured by law-enforcement agencies other than by interception is admissible in court. This subjects the intelligence to due legal process as admissible evidence and therefore the law-enforcement agency must ensure the evidence has been accessed lawfully – and meets the conditions of necessity and proportionality – for the Crown Prosecution Service to be able to bring a case and, subsequently, secure a conviction. If the evidence does not hold up to scrutiny there is a risk of the case collapsing or not making it to trial in the first place. The law of evidence – the procedures that govern proof of fact in legal proceedings – can act as a powerful constraint on law-enforcement agency actions, thereby acting as a check on law-enforcement surveillance.

4.46 Some civil-liberties groups have suggested that the current UK system of oversight has no judicial input.[29] 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 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.[30] 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

28. *Ibid.*
29. Big Brother Watch submission to the ISR; 'Apart from the authorisation of RIPA warrants at a local government level, there is no input from judges', p. 9.
30. In this regard, it is worth emphasising that the Rt Honourable Igor Judge was appointed as Chief Surveillance Commissioner from July 2015. Lord Judge is a former Lord Chief Justice for England and Wales, a 'critical constitutional role' as head of the judiciary. See Prime Minister's Office, 'Chief Surveillance Commissioner Appointment', press release, 20 March 2015.

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.

The Commissioners

4.47 The commissioners were introduced under a number of pieces of legislation, including the Interception of Communications Act 1985, SSA 1989, ISA 1994 and RIPA 2000. There are currently five commissioners in total, responsible for oversight of the interception of communications; the intelligence services; information; surveillance; and surveillance cameras. 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.[31] 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.

The Interception of Communications Commissioner

4.48 IOCCO is required to keep under review 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 with the ability to intercept communications. The IOCCO office features a team of nine inspectors drawn from a wide variety of backgrounds. The office conducts twice-yearly inspections of interception agencies and the government departments which authorise interception warrants, in addition to periodic visits. The 2014 annual report by IOCCO noted that it conducted twenty-six inspections, and made seventy-five recommendations to the nine interception agencies and four warrant-granting departments to improve compliance, and to improve systems and procedures for the interception of communications or the acquisition of communications data.[32]

4.49 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 Part I, Chapter I and that all relevant records have been kept
- All interception has been carried out lawfully and in accordance with RIPA Part I, Chapter I and its associated Code of Practice

31. Information Commissioner's Office (ICO) et al., 'Surveillance Road Map: A Shared Approach to the Regulation of Surveillance in the United Kingdom', Version 3.3, 2015.
32. Anthony May, *Report of the Interception of Communications Commissioner: March 2015* (London: The Stationery Office, 2015).

- Any errors are reported to the commissioner and that the systems are reviewed and adapted where any weaknesses or faults are exposed.[33]

4.50 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'.[34]

4.51 The inspections are also an opportunity for IOCCO to verify the warrant applications for errors; its office operates a breaches and error reporting function to which public authorities, CSPs and Internet companies are obliged to report any errors or breaches for investigation.

4.52 IOCCO has responsibility for the oversight of any interception of communication in the course of transmission carried by submarine cables. It examines the approvals to conduct the interception, the surveys that have been conducted by the engineers in relation to the material carried by those cables, and what percentage of the material is of intelligence interest. In its 2014 report it was also revealed that the commissioner had accepted a request from the prime minister to oversee (on a non-statutory basis) directions issued under Section 94 of the Telecommunications Act 1984.[35]

4.53 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.[36]

4.54 In total, 2,795 interception warrants to access the content of communications were authorised in 2014, an increase of 1.3 per cent on 2013. There were 1,605 extant warrants on 31 December 2014, a 3.8 per cent decrease on 2013. Of these, twenty were issued under Section 8(4), allowing for the collection of communications in large

33. Interception of Communications Commissioner's Office (IOCCO), 'Interceptions Inspections', <http://www.iocco-uk.info/sections.asp?sectionID=2&chapter=3&type=top>.
34. May, *Report of the Interception of Communications Commissioner: March 2015*, p. 2.
35. *Ibid.*, Section 10. Section 94 of the Telecommunications Act 1984 had previously come under criticism for allowing a Secretary of State to issue a direction in 'the interests of national security or relations with the government of a country or territory outside the United Kingdom' but without necessarily having to lay the direction before Parliament.
36. ISR round-table with the Commissioners, February 2015.

volumes where the sender and/or recipient are located overseas. The 'vast majority' of interception warrants do not run for more than six months. A sample of 936 warrants was specifically examined, amounting to 58 per cent of the number of extant warrants (34 per cent of the total of new warrants issued in 2014). Sixty-eight per cent of warrants were issued under the statutory purpose of preventing or detecting serious crime, 31 per cent were issued for national-security purposes and 1 per cent issued under both.

4.55 In 2014, 517,236 authorisations and notices under Chapter II, Part I of RIPA 2000 were made (excluding urgent oral applications). This was a slight increase on 2013 (514,608) but still significantly less that the 2012 figure (570,135). 88.9 per cent of authorisations and notices were made by the police and law-enforcement agencies, compared to 9.8 per cent by the intelligence agencies and 1.3 per cent for local and other public authorities.

4.56 Sixty interception errors were reported to IOCCO in 2014, with full details of all errors reported by both the interception agencies in question and the CSPs. Most related to safeguard breaches relating to RIPA 2000 Section 15/16, a failure to cancel interception, or interception of the incorrect communications address.

4.57 The majority of the commissioner's recommendations in the 2014 annual report fall into three key categories: the warrant application process, Section 15/16 safeguards, and the issue and implementation of warrants. Eleven specific recommendations were made to the interception agencies to 'review or shorten their retention periods and/or destroy interception material and/or related communications data where there was no persuasive justification provided for its on-going retention'. All recommendations were accepted and the large majority had already been implemented at the time of the report's publication, causing 'a significant amount of intercepted material and related communications data to be destroyed'.[37]

The Intelligence Services Commissioner

4.58 The primary role of the Intelligence Services Commissioner (InSeC) is to provide independent external oversight of the use of intrusive powers, interference with property, and investigation of electronic data protected by encryption by the intelligence agencies and parts of the Ministry of Defence. InSeC is also charged with keeping the following under review:

- The exercise by the secretaries of state of their powers to issue warrants and authorisations to enable the intelligence services to carry out their functions
- The exercise and performance of the powers and duties imposed on the intelligence services and Ministry of Defence and armed-forces personnel in relation to covert activities which are the subject of an internal authorisation procedure

37. May, *Report of the Interception of Communications Commissioner: March 2015,* p. 33.

- The carrying out of any aspect of the functions of the intelligence services as directed by the prime minister.[38]

4.59 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.[39] 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 InSeC also conducts under-the-bonnet inspections to review how warrants are put into operation.

4.60 During visits, the InSeC meets with the officers who wrote the submissions and cross-examines them on their justifications. He or she will sit with them at their desks to look at exactly what they are doing and how they think about privacy. Training regimes and training sessions are also inspected. Ethical guidance is examined, and particularly the avenues that are open to employees who may wish to raise concerns with someone other than their line manager. Any deliberate avoidance of due procedure would warrant a criminal investigation; though to date, no InSeC has found any evidence of this ever occurring.

4.61 In its 2013 annual report, the InSeC considered whether an unlawful warrant or authorisation could, in theory, be successfully issued.[40] Its conclusions were that this 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 warrantry 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).

4.62 Under the Justice and Security Act 2013, provision was made to expand the remit of the InSeC to include an ability to oversee, at the direction of the prime minister, any

38. Mark Walker, *Report of the Intelligence Services Commissioner for 2013* (London: The Stationery Office, 2014.
39. 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 (ISR round-table with the Commissioners, February 2015).
40. Walker, *Report of the Intelligence Services Commissioner for 2013* (London: The Stationery Office, 2014), p. 12.

other aspect of security and intelligence agency business.[41] In March 2015, the InSeC accepted an additional review function at the request of the prime minister to 'keep under review the acquisition, use, retention and disclosure [by the intelligence agencies] of bulk personal data sets, as well as the adequacy of safeguards against misuse'.[42]

4.63 Directed surveillance – such as a camera operated by MI5 and targeted at a specific person – would be an issue for the InSeC on the basis that it concerns surveillance by a security and intelligence agency directed at specific individuals. Whatever the actual technology used, intrusive methods are under the supervision of the commissioner. Authorisation for such directed surveillance would be done by a senior figure at the relevant agency who is outside of the operational chain of command for the investigation.

4.64 In 2013, 1,887 warrants and authorisations were approved across the intelligence services and the Ministry of Defence. The InSeC scrutinised 318 extant warrants and their supporting paperwork, representing 16.8 per cent of the total. The total number of new warrants and authorisations for 2013 was a reduction on 2012 (2,838). However, the statistics in the 2012 report have been described as misleading, as a number of authorisations were cancelled and then re-authorised as a result of their migration onto a new electronic system.[43]

The Office of Surveillance Commissioners

4.65 The statutory responsibility of the Office of Surveillance Commissioners (OSC) is to oversee the use of covert surveillance (property interference, intrusive surveillance and directed surveillance) and CHIS by all designated public authorities, with the exception of the SIAs (since this duty is carried out by InSeC). The OSC also has responsibility for overseeing RIPA 2000 Part III on access to protected data. Since January 2014, the OSC has looked at the use and authorisation of undercover operatives; the OSC will now grant (or deny) approval for any CHIS that has been deployed for longer than one year.

4.66 The OSC has a team of seven surveillance inspectors that undertakes annual inspections of all the law-enforcement agencies and triennial review of all other public authorities, local authorities and government departments.

4.67 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

41. See legislation.gov.uk, 'Justice and Security Act 2013, Explanatory Notes', < http://www.legislation.gov.uk/ukpga/2013/18/notes>.
42. See the Regulation of Investigatory Powers Act 2000, Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015.
43. Walker, *Report of the Intelligence Services Commissioner for 2013,* p. 35.

(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.

4.68 According to the OSC's 2013–14 annual report, 2,689 authorisations for property interference were granted during this period, an increase of 249 on the previous year (no applications were denied by the commissioners). 392 intrusive surveillance authorisations were made, an increase of twenty (the commissioners denied two authorisations). There was a significant increase in urgent authorisations, which were used on 1,032 occasions; this, however, still only represents around 5 per cent of the total number of authorisations granted.[44] Directed surveillance was authorised on 9,664 occasions, with 1,484 extant on 31 March 2014. This was an increase on the previous recording period when 9,515 authorisations were made with 1,118 extant. Directed surveillance authorisation by other public authorities continued to decline – from 5,827 in 2012–13 to 4,412 in 2013–14.[45]

4.69 In total, 4,377 CHISs were authorised by policing and law-enforcement agencies. 3,523 were cancelled within the 2013–14 reporting period, which included some who may have already been authorised in previous years. On the 31 March 2014, 3,025 remained authorised. Very few other public authorities use CHISs (3.7 per cent), and fifty-three remained authorised at the end of March 2014.[46]

The Information Commissioner's Office

4.70 The Information Commissioner's Office (ICO) has responsibility for promoting and enforcing the DPA 1998 and the FOIA 2000, along with associated legislation such as the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PEC Regulations).

4.71 ICO's goal is to achieve a society in which:[47]

- All organisations which collect and use personal information do so responsibly, securely and fairly
- All public authorities are open and transparent, providing people with access to official information as a matter of course
- People are aware of their information rights and are confident in using them

44. Christopher Rose, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2013–2014* (London: The Stationery Office, 2014), p. 10.
45. *Ibid.*, p. 11.
46. *Ibid.*, p. 13.
47. Christopher Graham, *Information Commissioner's Annual Report and Financial Statements 2013/14: Effective, Efficient – and Busier Than Ever* (London: The Stationery Office, 2014).

- People understand how their personal information is used and are able to take steps to protect themselves from its misuse.

4.72 The ICO also has some oversight of the Data Retention Regulations 2014, in light of a requirement to audit compliance with requirements and restrictions relating to the 'integrity, security or destruction' of data retained by CSPs. Since the 2006 report on the Surveillance Society prepared for the ICO,[48] the commissioner has been engaged in dealing with some of the issues raised around safeguards for privacy and effective regulatory oversight, not only in the context of intelligence and surveillance issues, but also in terms of the use of data by commercial organisations.

4.73 The ICO believes that it is for Parliament to decide what an oversight regime should look like, and sees effective oversight and redress as being absolutely essential for public trust and confidence.[49]

4.74 The ICO can report serious wrongdoing to the police, and has limited powers of sanction. In 2013–14, the ICO issued civil monetary penalties against a number of public and private authorities for failing to keep personal data secure – including Glasgow City Council, Nationwide Energy Services, NHS Surrey and the Ministry of Justice.

Figure 6: Reasons for Complaints to the Information Commissioner's Office.[50]

	2012–13 (%)	2013–14 (%)
Subject access	47	50
Disclosure	19	17
Inaccurate data	16	15
Security	6	6
Fair processing	2	2
Use of data	3	2
Right to prevent processing	2	2
Retention of data	1	1
Obtaining data	2	1
Excessive/irrelevant data	1	1

48. Surveillance Studies Network, 'A Report on the Surveillance Society', Summary Report, 2006.
49. Information Commissioner's Office submission to the ISR.
50. Graham, *Information Commissioner's Annual Report and Financial Statements 2013/14*, p. 14.

The Surveillance Camera Commissioner

4.75 The Surveillance Camera Commissioner (SCC) was introduced under the Protection of Freedoms Act 2012 with its role predominantly focused on raising awareness of, and generating debate on, the use of CCTV in public spaces and other related issues. The Act itself charges the commissioner to carry out three functions:

- To encourage compliance with the Surveillance Camera Code of Practice
- To review the operation of the code
- To provide advice about the code (including changes or breaches to it).

4.76 The SCC works very closely with the ICO due to the data principles incorporated in the Protection of Freedom Act. It is often difficult to determine the boundary with CCTV; while some CCTV issues are clearly the responsibility of the SCC, there are broader data-protection issues related to CCTV which were not anticipated by the Protection of Freedoms Act.

4.77 The SCC has no powers of inspection, enforcement or sanction; rather, the commissioner works with relevant authorities to make them aware of their duties with regard to the Surveillance Camera Code of Practice. The SCC has been charged with advising ministers during the course of this year on the findings of his first year in office, and particularly his assessment of the state of public-space CCTV and the compliance of those that fall within the Act. This will also include whether or not the commissioner believes it is correct for the role to have no sanctioning powers, and if the position of the SCC itself should be reviewed.

Strengthening the Commissioners

4.78 The varied focus of the commissioners and the occasional overlap in their activities reflect the different legislation introduced over time defining each of their different roles and responsibilities. This has created a regime in which some commissioners are focused on institutions (InSeC) and some on techniques (for example, the interception of communications).

4.79 The commissioners are aware that they must be careful not to become advisory bodies in addition to oversight and sanctioning bodies. IOCCO has raised concerns over agency officials coming to it before they apply for warrants to check whether they are doing it correctly. This can be a fine line; the agencies cannot seek a commissioner's advice in advance to ensure that they secure a warrant, but they are right to raise potential areas of concern in advance. Ultimately, it will always depend on individual circumstances.[51]

4.80 The current Intelligence Services Commissioner, Interception of Communications Commissioner and the Chief Surveillance Commissioner are all former senior judges

51. ISR round-table with the commissioners, February 2015.

and none of them had previously raised questions over the legality of legislation or the suitability of existing safeguards.

4.81 The Home Affairs Committee has encouraged the commissioners to actively consider issues of privacy, and has recommended more regular post-legislative scrutiny. Although the commissioners are of unquestionable ability and integrity, they are judges, not investigators. They are used to weighing up two sides of an argument and providing a ruling, but are generally less experienced in identifying problems of process or the application of new technology.

4.82 Evidence to the ISR Panel suggested that the commissioners need to be 'inquisitive troublemakers', with a level of investigatory expertise that is prized by the agencies themselves. There is a need for individuals with good analytical skills who can pick holes and identify weaknesses, as well as question and challenge people and practices within the relevant organisations. Given the depth of investigations, a common observation made to the ISR Panel was that the commissioners require greater assistance from teams of people with appropriate skills and expertise, perhaps in the form of legal and technical 'juniors'. (The same could be said of the IPT, which does not have permanent resources on technical matterson which it can draw.)

4.83 A final criticism highlighted to the ISR Panel relates to sanctions. Some of the commissioners have powers to impose civil monetary penalties (including the ICO and IOCCO). On the whole, however, the commissioners have relatively limited powers of sanction other than public opprobrium through their annual reports. However, in his 2015 report, IOCCO noted that 'there is always going to be certain information that I cannot reveal publicly' as his office is 'constrained by the statutory provisions in section 19 of RIPA 2000 forbidding disclosure, as are the interception agencies and Communication Service Providers'.[52]

The Investigatory Powers Tribunal

4.84 A Tribunal 'for the purposes of investigating complains about the [Security] Service' was originally legislated for under the SSA 1989. However, until RIPA 2000 was created eleven years later, the three original Tribunals (Interception of Communications, Security Service and Intelligence Services) had a very low profile and limited abilities. RIPA 2000 replaced the three Tribunals and the complaints provision of the Police Act 1997, Part III with the new IPT.[53]

52. May, *Report of the Interception of Communications Commissioner: March 2015*, p. 1.
53. Investigatory Powers Tribunal, 'Investigatory Powers Tribunal Report 2010', 2010.

4.85 The independent IPT was set up to consider complaints against the SIAs, particularly in light of the HRA 1998. The Tribunal investigates and determines two types of application:

- Interference complaints against a broad range of public authorities using covert techniques regulated under RIPA. A complaint can be about any interference that the claimant believes has taken place against them. This includes interception, surveillance and interference with property. The public authorities include UK intelligence, military and law-enforcement agencies as well as a range of government departments, regulators and local authorities
- Human-rights complaints. Claims can relate to the use of covert techniques by intelligence, military and law-enforcement agencies and to a wider range of human-rights breaches the claimant believes have been committed by the intelligence agencies.[54]

4.86 There is no right of appeal on the Tribunal's decisions, other than to go to the European Court of Human Rights. This presents a dilemma of the British government being bound by the rulings of the supranational ECtHR as a higher court, despite appeals being heard on the basis of less evidence – the British intelligence and security services will not submit to foreign judges sitting at the ECtHR the same material they would submit to the IPT, even if the Court were willing to consider evidence in secret. Any ECtHR hearing would therefore have to proceed on the evidence available and presumed fact, which might actually weaken the British government's case and prevent it from providing factual details and background to cases.[55]

4.87 Evidence to the ISR Panel indicates that the IPT is a work in progress. The commissioners can identify errors in their inspections, but have no legal basis on which to refer files to the IPT (despite their best efforts). Under Section 19 of RIPA, the content of interception warrants cannot be disclosed, even by the commissioners, so they are unable to notify the subject of wrongful interception in cases where this can be done without harming the public interest.

4.88 Cases at the IPT therefore have in the past tended to be triggered by individuals or organisations that have felt unjustly under surveillance. Information disclosed by Snowden has also triggered civil-liberties organisations to take a number of cases to the IPT. However, simply responding to accusations is not a helpful or just arrangement for either party. In order to be effective, the system must be able to regularly 'self-correct' by resolving any errors or injustices openly in court.[56]

4.89 Only select rulings are published by the IPT. In the past, as one academic has framed it, the procedures of the IPT were often opaque and did not 'accord with standards

54. Investigatory Powers Tribunal, 'Functions – Key Role', <http://www.ipt-uk.com/section.aspx?pageid=1>.
55. ISR legal round-table, March 2015.
56. *Ibid.*

of fairness that we require in other courts and tribunals, including those determining matters which touch on national security (such as control orders and now TPIM hearings). Where complaints are rejected … claimants are not given proper reasons but instead the judicial equivalent of a 'neither confirm nor deny' notice'.[57]

Recent Rulings

4.90 Assessments of the effectiveness of the IPT have been mixed in recent months, as a result of a number of high-profile rulings. The IPT has gone to some lengths to justify the procedures it has adopted to ensure that, although key information it needed to reach a judgment was highly classified and could not be revealed publicly, it was subject to proper scrutiny by Counsel to the IPT. Cases have also highlighted current weaknesses in the system.

4.91 In 2015 in *Liberty & Others vs. the Security Service, SIS, GCHQ*,[58] the IPT censured GCHQ for failing to provide enough detail on the safeguards on how it shared data with US counterparts until December 2014,[59] although it had previously ruled in December 2014 that the UK intelligence-collection methods did not breach the ECHR.[60] After two additional paragraphs of detail were made public, the agencies were found to no longer have been in contravention of human-rights law. [61]

4.92 In April 2015, the IPT ruled in favour of one claimant in a case that examined the potential interception by the intelligence agencies of legal professional privilege material involving eight Libyan plaintiffs (commonly referred to as the Belhaj case). This arose in the course of a case alleging complicity by the UK in the torture and rendition of the claimants to Libya.

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 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 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.

57. Moore, 'RIP RIPA?', pp. 128–29.
58. Investigatory Powers Tribunal, *Liberty & Others vs. the Security Service, SIS, GCHQ, IPT/13/77/H*, 5 December, 2014.
59. Investigatory Powers Tribunal, 'Approved Judgment', *Liberty & Others vs. the Security Service, SIS, GCHQ*, IPT/13/77/H, 6 February, 2015.
60. Investigatory Powers Tribunal, 'Approved Judgment', *Liberty & Others vs. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December, 2014.
61. Investigatory Powers Tribunal, 'Order', *Liberty & Others vs. the Security Service, SIS, GCHQ, IPT/13/77/H*, 6 February, 2015.

4.94 The ISR Panel note two particular concerns that arise from the case. The first is that the IPT could have made such a significant error, pointing to clear procedural improvements that will need to be implemented. A second concern is that the case represents a more systemic weakness of the IPT, in that errors only come to light after claimants make an application to the Tribunal, rather than through the established oversight mechanisms of the commissioners or ISC.

Ministerial Oversight

4.95 Ministerial accountability for the intelligence services is provided by the SSA 1989 and ISA 1994 and specifically by authorisation of warrants by secretaries of state under RIPA 2000. Under specific conditions (as not all surveillance activity requires a secretary of state-signed warrant), they provide the final level of pre-activity authorisation.

4.96 All warrants will have gone through an assessment by both the submitting agency and the receiving government department,[62] including by legal counsel, before reaching the secretary of state for approval.[63] However, even if a request is necessary, proportionate and legally sound, it may still be rejected on the basis of a political risk assessment. The number of refused requests is not currently published.

Parliamentary Oversight: The Intelligence and Security Committee

4.97 The ISC was first established by the ISA 1994 to examine the expenditure, administration and policy of the three British security and intelligence agencies. The ISC was reformed under the Justice and Security Act 2013 to make it a Committee of Parliament and to provide greater powers and the legal obligation for the agencies to provide material to the Committee. The statutory remit of the ISC was also expanded to include:

- A role in overseeing the wider government intelligence community (beyond the three security and intelligence agencies)
- Retrospective oversight of the operational activities of the agencies on matters of significant national interest
- Powers to require information from the agencies, subject only to a veto by the secretary of state rather than agency heads as was the case under the ISA 1994.[64]

4.98 In addition to the three intelligence and security agencies, the ISC now examines the intelligence-related work of the Cabinet Office including the JIC, the Assessments Staff and the National Security Secretariat. The Committee also provides oversight of Defence

62. Even urgent requests will go before at least two other people before reaching the secretary of state.
63. For example, in the FCO the Intelligence Policy Unit head sees approximately 95 per cent of submissions but some particularly sensitive requests will go straight to the director general, defence and intelligence; ISR visit to the FCO, March 2015.
64. Legislation.gov.uk, 'Justice and Security Act 2013, Explanatory Notes'.

Intelligence in the Ministry of Defence and the Office for Security and Counter-Terrorism (OSCT) in the Home Office. Committee members are subject to Section 1(1)(b) of the Official Secrets Act 1989 and have access to highly classified material in carrying out their duties. The Committee takes evidence from Cabinet ministers and senior officials – all of which is used to formulate its reports.[65]

4.99 Members of the ISC are appointed by Parliament from across both the Commons and Lords after nomination by the prime minister, and the Committee reports directly to Parliament. It is therefore a statutory committee, rather than a parliamentary select committee (members of which are nominated and elected by Parliament). Parliament was given a more substantial role in ISC appointments under the Justice and Security Act 2013.

4.100 The ISC does not investigate individual complaints about the security and intelligence agencies, or allegations that their intrusive powers have been used unlawfully. Such matters are referred to the IPT. However, shortly after the Snowden disclosures began in June 2013, the ISC released a statement on GCHQ's alleged interception of communications under the US PRISM programme,[66] followed by a complete special report in 2015, 'Privacy and Security: A Modern and Transparent Legal Framework'.

4.101 The Committee has been criticised in the past for being chaired by individuals having previously had a close relationship with the agencies: Sir Malcolm Rifkind (former foreign secretary); Lord King (former defence secretary); and Paul Murphy (former secretary of state for Northern Ireland). Dr Kim Howells (former minister of state for foreign and commonwealth affairs) and Baroness Taylor (former minister for international defence and security) are the only former chairpersons not to have had any involvement with the agencies prior to their appointment to the ISC, yet Baroness Taylor was also criticised at the time of her appointment for lacking necessary experience and qualifications.[67]

4.102 The Committee has also been criticised for not providing rigorous enough oversight of the SIAs, and for having a cosy rather than arm's-length relationship with the agencies it oversees. According to testimony from some of the commissioners, there is evidence to indicate a lack of constructive and substantive relationship between the commissioners and the ISC, with the ISC showing a lack of interest in exchanging views.[68] The ISR Panel recommend that there is substantially improved engagement between the commissioners and ISC to ensure as thorough an oversight process as possible.

65. ISC, 'About the Committee', <http://isc.independent.gov.uk/home>.
66. ISC, 'Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme', 2013.
67. Matthew Tempest, 'Lib Dems Criticise Taylor Appointment', *Guardian*, 2 August 2011.
68. ISR round-table with the commissioners, February 2015.

V. A Democratic Licence to Operate

5.1 While the ISR was initiated following the disclosures by Edward Snowden, the Review reflects a wider and longstanding debate in the UK surrounding the interception of communications, internet surveillance and state intrusion into privacy. Rather than representing a spectrum of opinion, this debate has often been framed in terms of individual privacy versus collective security.

5.2 On the 'security' side, the police and SIAs argue that, in order to stay one step ahead of increasingly capable adversaries, they must have a particular set of advanced and potentially intrusive capabilities. On the 'privacy' side, civil-liberties and privacy advocates believe that the capabilities of the agencies are disproportionate to the threat, and that the oversight mechanisms that hold them to account are inadequate.

5.3 It was within this context that the disclosures by Edward Snowden emerged. The information brought sharp focus to the debate and entrenched positions on both sides. Allegations of bulk data collection raised specific legal questions on the remit and oversight of the SIAs in many countries, including the UK.

5.4 The ECJ ruling in *Digital Rights Ireland* – declaring invalid the EU Data Retention Directive – marked a significant moment. According to the UK government, the subsequent introduction of DRIPA 2014 was designed to resolve the immediate potential loss of capability; the sunset clause, meaning the legislation will cease to have effect from the end of 2016, would allow time to conduct a more thorough review of the intrusive powers required by the agencies, as well as the legislation regulating these powers.

5.5 The ISR report is one of three reports whose findings will be drawn upon to inform the government's approach in this regard and also future legislation. In June 2015, Theresa May acknowledged that the government would be giving due consideration to all three reports in parallel:

> These independent reviews are each important and valuable contributions to the continuing debate about the role of our security, intelligence and law enforcement agencies, their use of investigatory powers and their oversight. The Government will need to give proper consideration to their recommendations, but I believe that collectively they will provide a firm basis for consultation on legislation.[1]

1. Theresa May, *Hansard*, House of Commons Debates, Col. 1353 (11 June 2015).

The ISC Inquiry

5.6 In July 2013, the ISC issued a statement on the specific media allegations over the activities of GCHQ, and its subsequent investigation. It noted that 'While some of the stories are not surprising, given GCHQ's publicly acknowledged remit, there is one very serious allegation amongst them – namely that GCHQ acted illegally by accessing communications content via the PRISM programme'.[2] After investigation, the ISC concluded that GCHQ had not circumvented UK law.

5.7 The ISC also concluded, however, that there were wider issues of concern. In particular, it noted that 'some elements of the legislative framework governing the Agencies' work are overly complex, difficult to interpret in relation to certain internet technologies, and lack transparency'.[3] It announced that it would therefore be initiating a full inquiry to 'consider further whether the current statutory framework governing access to private communications remains adequate'.[4] In October 2013, it confirmed that it would be broadening its inquiry to also consider the 'appropriate balance between our individual right to privacy and our collective right to security'.[5]

5.8 The ISC published a redacted version of its report in March 2015. As its title ('Privacy and Security: A Modern and Transparent Legal Framework') suggests, the primary focus of the report was on the 'opaque' and 'unnecessarily complicated' myriad of legislation governing the activities of the agencies. Its key recommendation was therefore that 'the current legal framework be replaced by a new Act of Parliament governing the intelligence and security Agencies. This must clearly set out the intrusive powers available to the Agencies, the purposes for which they may use them, and the authorisation required before they may do so'.[6]

5.9 On the issue of the authorisation of warrants, the primary question the Committee considered was whether ministers or judges should sign warrants for intrusive activity. Recognising concerns over public trust in politicians, the ISC nevertheless concluded that 'the most intrusive activities must always be authorised by a Secretary of State'.[7] The basis for this decision was that ministers are able to make a judgement of the diplomatic and political context and the wider public interest in authorising intrusive powers, in addition to assessing legal compliance. The Committee also considered it crucial that, unlike judges, ministers are politically accountable for their decisions.

---

2. Intelligence and Security Committee of Parliament (ISC), 'Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme', 2013.
3. ISC, *Privacy and Security: A Modern and Transparent Legal Framework* (London: The Stationery Office, 2015), p. 11.
4. ISC, 'Statement on GCHQ's Alleged Interception of Communications'.
5. ISC, 'Privacy and Security Inquiry – Call for Evidence', 11 December 2013.
6. ISC, *Privacy and Security,* p. 2.
7. *Ibid.*, p. 119.

5.10 With regards to the capabilities of the SIAs, the Committee found that 'GCHQ's bulk interception is a valuable capability that should remain available to them',[8] and was satisfied that 'current legislative arrangements and practice are designed to prevent innocent people's communications being read'.[9] However, it also acknowledged that 'the time has come for much greater openness and transparency regarding the Agencies' work'.[10] In this vein, the report avowed intrusive capabilities of the SIAs that had previously only been 'implicitly authorised' under existing legislation, such as the use of ICT operations against targets overseas and the acquisition of bulk personal data sets.

The Investigatory Powers Review

5.11 As part of the unveiling of DRIPA 2014 in July 2014, the home secretary announced that the independent reviewer of terrorism legislation, David Anderson QC, would be appointed to review the operation and regulation of investigatory powers. The review was given statutory force in Section 7 of DRIPA 2014.

5.12 Under his terms of reference, Anderson was asked to look at whether or not the UK required new legislation and, in particular, whether Part 1 of RIPA 2000 (which deals both with interception and with communications data) needed to be amended or replaced. He was also tasked to examine transparency requirements and the effectiveness of current statutory oversight arrangements.

5.13 Anderson delivered his report to the prime minister in May 2015, and the government published it in full in June. Anderson is critical of RIPA 2000, describing it as 'obscure since its inception', having been 'patched up so many times as to make it incomprehensible to all but a tiny band of initiates. A multitude of alternative powers, some of them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and – in the long run – intolerable'.[11] Anderson agrees with the ISC that a 'comprehensive and comprehensible new law should be drafted from scratch, replacing the multitude of current powers and providing for clear limits and safeguards on any intrusive power that it may be necessary for public authorities to use'.[12]

5.14 One of the most radical recommendations in the report, as the author himself acknowledges, was that all warrants (including a new type of 'bulk warrant') should be authorised by judicial commissioners, rather than the secretary of state. Noting that secretaries of state are rarely, if ever, held politically accountable for the issue of warrants, Anderson believes that a system of judicial warrants would help improve public confidence. Having taken evidence from a number of US companies, he also suggests this

8. *Ibid*., p. 33.
9. *Ibid.*, p. 112.
10. *Ibid.*, p. 120.
11. David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* [Anderson Report] (London: The Stationery Office, 2015), p. 8.
12. *Ibid.*, p. 4.

would facilitate obtaining assistance from service providers in the US, who stated that they were more accustomed to the procedures of the Foreign Intelligence Surveillance Court and disliked the notion of authorisation by the secretary of state.[13]

5.15 In cases where the warrant is required in the interests of the defence and/or foreign policy of the UK, Anderson suggests the warrant would be sent first to the secretary of state, who would certify that this was the case. The judicial commissioner would only be able to depart from that certification on the basis of judicial review. The advantage of this dual system, Anderson believes, is that 'it would preserve the proper role of the Secretary of State in relation to the assessment of the defence and foreign policy priorities of the country', while the judicial commissioner would still 'retain the ability to scrutinise such warrants for compliance'.[14]

5.16 In order to increase confidence in the oversight regime, Anderson recommends that the judicial commissioners be housed in a new Independent Surveillance and Intelligence Commission. The Commission would also bring together, merge and add to a number of the oversight responsibilities held by the Interception of Communications Commissioner's Office, the Office of Surveillance Commissioners and the Intelligence Services Commissioner.[15] The Commission would be public-facing and draw on expertise from a range of sectors, including intelligence, computer science, technology, academia, law and the NGO sector.

A Democratic Licence to Operate

5.17 The ISR Panel have considered in detail each of these reports, and their significant number of recommendations in particular. Some, but not all, of their findings and recommendations reflect the Panel's own investigation. This investigation involved a thorough review of existing literature, seventeen evidence sessions, as well as meetings with, and visits to, thirty-eight organisations and individuals. These visits included government departments and agencies such as the FCO, the three British security and intelligence agencies (GCHQ, MI5 and SIS), the NCA and the Metropolitan Police.

5.18 Like the ISC and the IPR investigations, the Panel were impressed by the dedication and professionalism of the police and the intelligence services in the way they have approached the problems of intercepting communications and their use of data in the digital society. There is evidence of high levels of expertise among the individuals responsible for implementing the interception and use of data for security and policing purposes.

5.19 Welcome as such dedication is, the key questions lie much deeper. Open societies have to protect themselves, but the parts of the state entrusted with significant powers must be carefully regulated and held to a high level of accountability. If the first duty of

13. *Ibid.*, p. 207.
14. *Ibid.*, p. 274.
15. *Ibid.*, p. 299.

government is to protect its citizens, then there is some part of government in the open society that must nevertheless constitute the secret parts of the state. These parts of the state cover the intelligence services and many of the investigative functions of the police and other law-enforcement agencies. Their necessary secrecy and the considerable power they have to intrude into the lives of citizens means that the secret elements of the state must be regarded as special, but subject to even more special constraints.

5.20 Much of the work of the secret parts of the state has to be handled with the utmost confidentiality or it simply fails to be effective. The vast majority of the information political leaders may need in the normal course of their policy-making is provided by open sources. But when they need to draw on secret information, nothing else will do. The concepts of transparency and accountability are often misunderstood in these discussions. It is unrealistic for the intelligence agencies and some specialist parts of the police service to operate in very transparent ways. They could not be effective if they did. They should, however, be rigorously and independently held accountable, and the oversight mechanisms must themselves be highly transparent to the public. This is an investment in public trust, without which the secret parts of the state cannot be effective or even legitimately exist.

5.21 It is therefore understood that those special surveillance techniques and human skills of the intelligence agencies are only used to tackle the most difficult information-based tasks in the business of national security. Similar skills are required for the most demanding police tasks. The Panel recognise the importance of maintaining and updating these capacities in the face of rapid technological change. But these skills and techniques must be carefully constrained and should not be allowed to seep into other areas of government where their use is neither necessary nor appropriate. Care must be taken to ensure these skills are used in the public interest and not private or institutional interests. Additionally, secrecy must not be used as a means to avoid accountability or hide mistakes.

5.22 The Panel understand that advances in digital technologies have brought new challenges and pressures, particularly for law enforcement and national security. Technology enhances the lives of the vast majority of those using it, but the same capabilities are used by criminals and adversaries. Internet-based technologies are a powerful force multiplier both for good and bad; in particular, they increase the influence of non-state groups and organisations – as opposed to governments – on the lives of individuals. The digital society promises new expressions of individual freedom and democratic engagement. But the corresponding advantage for malign groups and individuals is a phenomenon to which modern Western governments are still trying to adjust.

5.23 This challenge to adjust is not only created by technological ‘flattening’ – the growing power of technologies widely available to individuals and private groups – but by the inherently global nature of internet-based technology. The Internet naturally crosses jurisdictional boundaries, but the agencies of government are, by definition, jurisdictional

and must operate from that starting point. Some international harmonisation of national legislation is essential. Any government thinking about its powers of intrusion must consider the reality that other governments take different views within their jurisdictions – from autocratic regimes which spy extensively on their own populations, to those who take a minimalist approach and do not feel themselves under undue pressure from international criminality, terrorism or malign nations.

5.24 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.

5.25 In light of this, it is not surprising that the Snowden disclosures sent ripples of anxiety through part of the country. The intelligence agencies have acknowledged this, saying to the Panel that 'the dials will have to be reset'. This is reflected in the government's programme to renew the legislative basis for the interception of communications during the current Parliament.

5.26 But the Panel believe that such 'resetting' of the dials must also be undertaken on the basis of some very clear principles. The Snowden disclosures have made it imperative that what was previously an essentially implicit bargain between government and citizens over the rights of intrusion into private life should be made explicit.

5.27 Given the speed of technological and social change within our open society, it is likely that every generation will have to look afresh at the licence it gives to the secret parts of the state. Technology will continue to make exponential leaps but the essential requirements of the open society will endure.

5.28 The state should always be reluctant to invade the privacy of its citizens in an open society; it should never be a matter of routine. It is something about which the secret parts of the state should rightly feel unease and which should test the professionalism of the individuals within it. Intrusions into privacy, interception of communications and the analysis and retention of data all require fine judgements which are seldom straightforward and should never be regarded as easy or simply uncontentious. The day the British state becomes casual about the way it uses its secret capacities will be the day for the most acute anxiety. The key test for an open society is how it constrains and confines the secret parts of the state.

5.29 A new licence for the law-enforcement and security and intelligence agencies to operate for our generation must be based on a shared approach that would constitute an explicit

bargain on state surveillance and interception of communications. To be sustained, such a grand bargain would contain within it three distinct deals.

5.30 One deal is between the UK state and the citizen. The evidence in this Review indicates that the public in Britain is generally supportive of the work and expertise of the SIAs and of the requirements of intelligence-led policing. There has not been a strong popular outcry against the revelations of bulk data collection for intelligence purposes, though there is certainly evidence of some unease at the prospects of its misuse, whether by government or industry. There is certainly a problem of trust in the system of oversight, and particularly the lack of popular visibility of the oversight arrangements that currently exist. A clear and transparent new legal framework and a more coherent, visible and effective oversight regime should be the basis for a public discussion about the appropriate and constrained power the British state should have to intrude into the lives of its citizens. This would be the essence of a new deal between citizen and government.

5.31 The second deal would be a better shared understanding between the government, CSPs and internet firms. These companies should not be seen as disinterested observers as democratic governments try to square the circle between the security of the citizen and their right to privacy. Internet firms have a major stake in open societies. Without them, the Internet would not exist in its present form, and beyond complying with the law they have a responsibility to help sustain open societies even as the industry attempts to respond to customer concerns.

5.32 The third deal would be between the signatory states of the Convention on Cybercrime.[16] This would involve a process to spell out a common political goal among these countries, to reconcile democratic principles with the new political challenges posed by internet-based technology and to harmonise the different legal jurisdictions in this field as much as possible. This would transcend, but should be consistent with, the current EU framework.

5.33 The majority of these signatory states can be seen as a core of essentially democratic and open societies, whose agreement would have wider international impact. It would help mitigate concerns that intelligence-partnering arrangements could circumvent national law; that is, where material gathered under a different national legal jurisdiction might be shared. Common and explicitly adopted principles would make this less problematic and also reduce the scope for abuse of process by any of the individual countries.

5.34 If progress towards these three deals is possible, then the Panel believe that a new bargain can be struck that would be enduring in the face of unpredictable technological change and evolving legal frameworks. It is very unlikely that the new legal framework currently under discussion in Britain will be the last, and the questions this Review has tackled will be posed again in the future.

16. With the exception of Russia and San Marino, all forty-seven countries of the Council of Europe are signatories to the Convention, in addition to Australia, Canada, Japan, South Africa and the United States.

Ten Tests for the Intrusion of Privacy

5.35 We believe there are ten enduring tests that Parliament and the public should apply when considering all future legislation relating to the conditions under which the police and intelligence and security agencies can intrude upon the privacy of the citizen. They derive from principles we believe must be constantly observed and which encapsulate the most essential elements in the grand bargain we have outlined.

1. **Rule of law**: All intrusion into privacy must be in accordance with law through processes that can be meaningfully assessed against clear and open legislation, and only for purposes laid down by law.
2. **Necessity**: All intrusion must be justified as necessary in relation to explicit tasks and missions assigned to government agencies in accordance with their duly democratic processes, and there should be no other practicable means of achieving the objective.
3. **Proportionality**: Intrusion must be judged as proportionate to the advantages gained, not just in cost or resource terms but also through a judgement that the degree of intrusion is matched by the seriousness of the harm to be prevented.
4. **Restraint**: It should never become routine for the state to intrude into the lives of its citizens. It must be reluctant to do so, restrained in the powers it chooses to use, and properly authorised when it deems it necessary to intrude.
5. **Effective oversight**: An effective regime must be in place. Effectiveness should be judged by the capabilities of the regime to supervise and investigate governmental intrusion, the power it has to bring officials and ministers to account, and the transparency it embodies so the public can be confident it is working properly. There should also be means independently to investigate complaints.
6. **Recognition of necessary secrecy**: The 'secret parts of the state' must be acknowledged as necessary to the functioning and protection of the open society. It cannot be more than minimally transparent, but it must be fully democratically accountable.
7. **Minimal secrecy**: The 'secret parts of the state' must draw and observe clear boundaries between that which must remain secret (such as intelligence sources or the identity of their employees) and all other aspects of their work which should be openly acknowledged. Necessary secrecy, however, must not be a justification for a wider culture of secrecy on security and intelligence matters.
8. **Transparency**: How the law applies to the citizen must be evident if the rule of law is to be upheld. Anything 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.
9. **Legislative clarity**: Relevant legislation is not likely to be simple but it must be clearly explained in Codes of Practice that have Parliamentary approval, are kept up-to-date and are accessible to citizens, the private sector, foreign governments and practitioners alike.

10. **Multilateral collaboration**: Government policy on intrusion should be capable of being harmonised with that of like-minded open and democratic governments.

5.36 We believe that a state that continually and consistently applies these ten principles will not find itself in abuse of its duties to its citizens or veering towards the over-mighty. In the end, for an open society, the obtrusive powers held by the state can only be based on consent.

Conclusions

5.37 In the sections below, the ISR Panel outline their conclusions relating to what they consider to be the five most important themes of its review: bulk data collection and data retention; maintaining the capabilities of the SIAs and law-enforcement agencies; the warrantry system; the transparency of the oversight regime; and collaboration between the public and private sectors.

5.38 The ISC's and David Anderson's reports make some 150 recommendations. We agree with some but not all of them and are keen not to duplicate much of the good work that has already been done. Below are our key recommendations drawing on published reports, our visits to the police and SIAs and our evidence sessions at RUSI.

Maintaining the Capabilities of the Agencies

5.39 It was clear from the majority of the Panel's visits and evidence sessions that the digital era has created significant new challenges for the police, law enforcement and SIAs. They face a diffuse threat from a variety of capable and technology-literate adversaries operating across a number of different jurisdictions. The rapid development of ICT and Internet-based communications has challenged some of the traditional approaches, structures and processes developed by law-enforcement and intelligence agencies over decades.

5.40 In order to carry out their primary function of ensuring the safety and security of the British public, it is crucial that the agencies have the necessary powers. Given the degree to which they may intrude upon a citizen's privacy, it is right that these powers should be codified in law. This legislation should clearly set out the circumstances in which intrusive powers can be used, as well as the measures and safeguards in place to prevent abuse.

5.41 The Panel agree with both the ISC and the Anderson reports when they say that certain pieces of existing legislation are unclear. While it may be unnecessary to reform *all* legislation in this area (the SSA 1989 or ISA 1994, for example), there is a need to introduce new legislation governing the authorisation and use of intrusive powers, particularly as they relate to the interception of, and access to, digital communications.

5.42 This new legislation will need to clarify which public-sector organisations are able to use such powers. Building on the current criteria relating to the use of investigatory powers,

there is a reasonable public expectation that the interception of communications, broadly defined, should only be conducted in cases of national security, to prevent or detect serious and organised crime, or in certain other areas which would have to be closely defined and agreed by Parliament.

5.43 It is not possible to keep the public safe without law-enforcement agencies and SIAs having access to certain types of information. Bulk data collection is considered in more detail below, but there was agreement among Panel members that there should be provision to allow communications data to be retained by CSPs for a certain period of time and under specific conditions and safeguards, and that these agencies should be able to access it under legal and properly authorised circumstances.

5.44 Recognising the significant benefits that increased levels of encryption bring, the ISR Panel are also cognisant of the fact that sophisticated data encryption and increased use of end-to-end encryption by Internet firms will also have serious consequences for law-enforcement agencies and the SIAs.

5.45 We do not believe that the police, law-enforcement agencies and SIAs should have blanket access to all encrypted data, by legally requiring the handover of decryption keys, for example; however, in certain circumstances data should not be beyond the reach of the agencies. We agree with Anderson in his recommendation that in the digital world as in the real world, no-go areas for intelligence and law enforcement should be minimised. There should not be parts of the Internet or means of communication that criminals can use, but to which law enforcement are unable to seek access. For instance, it must be possible to seek access to evidence if it will help to convict a known criminal, or if it will protect the public from an imminent threat. Access may not always be guaranteed but there must, in principle, be a right to seek access in accordance with the principles the Panel have outlined.

5.46 In broader terms, new and emerging technological developments will continue to challenge the agencies and the way in which they operate. Ministers, civil servants and regulators all have a role to play in ensuring not only that the agencies remain within their remit in responding to these new challenges, but also that they have the appropriate capabilities and resources to do so.

5.47 We refer in Chapter III to the broader national challenge that digital technologies pose to the education and training of the population as a whole. There is no room for complacency and these challenges should be clearly acknowledged. The Panel are particularly concerned that levels of technical understanding among policy-makers and legislators are seriously deficient and the best use is not being made of the technical expertise already available. Support and advisory bodies, such as the Technical Advisory Board and Communications Data Steering Group, are not being exploited to their full potential. Government officials must have sufficient understanding of relevant technical issues to both assess the needs of the agencies and provide credible oversight of their activities.

Legislation

Recommendation 1: We support the view – as described in both the Intelligence and Security Committee of Parliament (ISC) and Anderson reports – that the current surveillance powers are needed but that they require a new legislative framework and oversight regime. We do not believe that the ISC's recommendation of consolidating all current laws relating to the intelligence agencies in a single legal framework is required to achieve substantial reform, nor do we think there should be separate legislation for the police and for the security and intelligence agencies. We agree with David Anderson's suggestion that RIPA 2000 Part I, DRIPA 2014 and Part 3 of the CTSA 2015 should be replaced by a comprehensive new law.

Recommendation 2: The new legislation should be clearly articulated while also recognising the complexity of the issues. Codes of Practice, published in statute, should be written in plain and accessible language and include details of implementation and technical application of the legislation.

Recommendation 3: Following evidence received by the ISR Panel and further discussion with civil-liberties groups and communications service providers (CSPs), we recommend that definitions of content data and of communications data should be reviewed as part of the drafting of new legislation. They should be clearly delineated in law.

Police, Law Enforcement and Local Authorities

Recommendation 4: While the number of public authorities with the power to obtain communications data has recently been reduced, we believe (i) that there should be a periodic review of which public bodies have the authorisation to use intrusive powers (such as directed surveillance and interception of communications) and (ii) that all relevant applications from authorised public bodies to obtain communications data must be made via the National Anti-Fraud Network as the national single point of contact in the future.

Recommendation 5: A national approach to policing in the digital era is necessary and long overdue. The police require a unified national digital policing strategy and the resources to deliver the capability to ensure digital investigations and intelligence capability. This will require a co-ordinated national effort bringing the relevant bodies together, and a review of core training in digital investigations and intelligence skills for all officers.

Advisory Council for Digital Technology and Engineering

Recommendation 6: A Technical Advisory Board was established under RIPA 2000 which brought together industry experts in a personal capacity. Since its inception, the Board has not met regularly and is seen as ineffectual. The government should replace the

Board with an Advisory Council for Digital Technology and Engineering. The Advisory Council would be a statutory and non-departmental public body established under new legislation. Terms of reference for a new Advisory Council should be drawn up so as to keep under review the domestic and international situation with respect to the evolution of the Internet, digital technology and infrastructure, as well as:

- Provide advice to relevant ministers, departments and agencies on technical measures
- Promote co-operation between the public and private sectors
- Manage complaints from CSPs on notices and measures they consider unreasonable
- Advance public education
- Support research on technology and engineering.

Recommendation 7: The Advisory Council should be a resource for a new National Intelligence and Surveillance Office (see Recommendation 17) and the ISC.

Bulk Data Collection and Retention

5.48 While the focus of much public concern relates to bulk data collection, the Panel believe it is important to distinguish between the relative impact on privacy of the processes of data collection, retention and analysis. Privacy issues need to be considered afresh at each stage.

5.49 The Panel are persuaded by the argument that the SIAs in particular will always need to conduct both targeted (that is, specifying the individuals or premises to be covered by the warrant) and untargeted data collection (recognising that even untargeted collection must be specifically aimed at achieving an authorised mission or intelligence requirement). Targeted data collection will be needed when the agencies have identified a subject or subjects of interest and require further information on them, if only to confirm whether or not they pose a threat. Some degree of untargeted data collection, involving the collection of data in bulk, may sometimes be required, especially given the nature of modern communications.

5.50 The Panel accept that some critics will remain convinced that untargeted data collection as a principle is unacceptable, and we recognise their concerns. At the same time, the Panel believe that the ability of the SIAs to collect data in bulk may in some instances be necessary when there is no viable alternative for them to identify potential and unknown threats, particularly online. However, the Snowden disclosures show how such data collection can be undertaken without public awareness or consent. Such awareness and consent are crucial, as are robust oversight mechanisms to reassure the public that capabilities are not being misused or abused. The Panel note that a number of improvements can be made to the current system of oversight to improve confidence, discussed in more detail below.

5.51 There are further concerns about what happens to an individual's data *after* it has been collected, in particular the circumstances in which this data is interrogated and analysed (explored in the warrantry-regime section below), and for how long data is kept.

5.52 From our evidence sessions, we heard that issues of data retention can also be controversial. As discussed in previous chapters, there are good reasons for which data may be retained and analysed (particularly since, at the point of collection, the true value of the data may not be known and it may take time to process the data to filter what is needed). However, this also raises the possibility of future mission creep, and that the data will be used for purposes other than that for which it was collected, violating well-established principles of data protection. The longer the data is held, the greater the risk of course that the data may be lost and/or stolen.

5.53 The Panel believe that such fears can be managed by improving oversight, and remain convinced there is a case for certain data to be retained within set timeframes, under certain conditions and subject to the requirements of data-protection law. Policies on data retention must be subject to regular review by oversight bodies to ensure they remain proportionate (and, as noted above, oversight mechanisms must have the technical knowledge to monitor this effectively).

Recommendation 8: The capability of the security and intelligence agencies to collect and analyse intercepted material in bulk should be maintained with stronger safeguards as set out in the Anderson Report. In particular, warrants for bulk interception should include much more detail than is the case currently and be the subject of a judicial authorisation process, save for when there is an urgent requirement (see Recommendation 10, point 2).

The Warrantry Regime

5.54 Warrants are an established and important legal mechanism authorising the use of intrusive powers. They are crucial in being able to monitor, record and audit the use of these powers. A number of aspects of the warrantry system are the subject of debate. Key questions we consider include: Who has the power to sign a warrant? What is the process and criteria for applying for warrants? How are warrants audited to ensure compliance, and by whom?

5.55 The Panel gave particular thought to the current warrantry system. We believe that any changes to the current system must ensure efficient and occasionally urgent processing, but with sufficient rigour of examination. The process must ensure consistency (such that the same input will produce the same decision) and must be scalable, particularly if the number of warrant applications increases.

5.56 The distinction between content data (the interception of which requires a warrant) and communications data (requiring an authorisation) remains relevant, but new definitions are required in legislation, particularly given the ever-growing volumes of

communications data now available. The Panel agree with the Anderson Report that it would be sensible to introduce a new type of warrant, covering the collection of communications data in bulk, in addition to the present ability to obtain warrants for access to content data in bulk.

5.57 Currently the most contentious issue is whether it is more appropriate for government ministers or judicial officials to authorise warrants (though there is universal agreement that judicial figures should *audit* warrant applications, as is currently the case). There are good, clear arguments on both sides, which have been set out in detail by both the ISC and the Anderson reports. In summary, these arguments tend to relate to issues of *trust* (it is widely held that judges inspire greater public confidence than ministers), *capability* (whether both parties are able to make legal assessments and judgements over political risk) and *accountability* (ministers are accountable to Parliament for their decisions, whereas a right to appeal exists for those dissatisfied with a judicial decision).

5.58 Under the current system, a distinction is made between a warrant granted under Section 8(1) of RIPA 2000, which must name or describe the subject of the interception, as well as the 'selectors' (such as an e-mail address, postal address, telephone number and so on) that will be used to identify the communications that are to be intercepted, and a warrant granted under Section 8(4) of RIPA 2000 that does not need to name the subject of interception, nor does it impose an express limit on the number of external communications which may be intercepted. Separately, it has been suggested a number of times to the Panel that the distinction between domestic and international communications is likely to become irrelevant in the Internet age. Likewise, we also believe that future legislation should distinguish more clearly between data in transmission and stored data.[17]

Recommendation 9: We agree with both the ISC and Anderson reports that there should be different types of warrant for the interception and acquisition of communications and related data, and have drawn on both sets of recommendations. We recommend three types of warrant for the interception of communications and an authorisation for communications data:

1. For the interception of communications in the course of transmission we suggest two different types of warrant:
   a. A *specific interception warrant* which should be limited to a single person, premises or operation
   b. A *bulk interception warrant* which would allow content data *and* related communications data to be obtained.
2. For the acquisition of communications data in bulk, a *bulk communications data warrant* which would be limited to the acquisition of communications data

17. The current view (as expressed in Edmondson & ors v R [2013] EWCA Crim 1026) is unclear, especially for e-mails that have been read and stored.

3. For the acquisition of communications data otherwise than in bulk, an *authorisation* by the relevant public authority. Communications data should only be acquired after the authorisation is granted by a designated person.

5.59 Secretaries of state and the judiciary both play an important role in the authorisation of intrusive powers. Judges are best suited to applying the necessary legal tests, but ministers are better informed about the nature of the threat and are best placed to assess necessity and proportionality as they relate to national security. Ministers are also in a better position to exercise political judgement over intelligence operations and therefore have a legitimate role in the management of the state's most intrusive powers.

5.60 Our starting point is that judicial commissioners should play a full role in the warrantry process rather than sampling some warrants *ex post* (as they do currently). This would mean appointing judicial commissioners on a full-time basis and who would be able to cater for urgent requests and therefore would require proper resources.

Recommendation 10: We recommend that the government adopts a composite approach to the authorisation of warrants, dependent on the purpose for which the warrant is sought and subsequent degree of ministerial input required. Our approach does not discriminate between whether it is law enforcement or an intelligence agency submitting the warrant.

1. Where a warrant (see points 1a, 1b and 2 in Recommendation 9) is sought for a purpose relating to the detection or prevention of serious and organised crime, the warrant should always be authorised by a judicial commissioner. Most police and other law-enforcement warrants would fall into this category. A copy of each warrant should be provided to the home secretary (so that the home secretary and officials can periodically examine trends in serious and organised crime, for example).
2. Where a warrant (see points 1a, 1b and 2 in Recommendation 9) is sought for purposes relating to national security (including counter-terrorism, support to military operations, diplomacy and foreign policy) and economic well-being, the warrant should be authorised by the secretary of state subject to judicial review by a judicial commissioner. The review should take place before implementation of the warrant. If there is a case of urgency the secretary of state should be able to direct that a warrant comes into force immediately, and the judicial commissioner should be notified straight away and the judicial review conducted within fourteen days.

The judicial commissioners in charge of the authorisation of warrants should not be part of a new National Intelligence and Surveillance Office nor should they be based in a government department, but alternative office facilities should be sought so that the commissioners are accessible but remain independent. To ensure no loss of

operational efficiency, appropriately qualified judges would have to be available at all times throughout the year.

The Transparency of the Oversight Regime

5.61 The Panel welcome the positive changes in approach of the SIAs during the time that we have been conducting this Review, and that more information is in the public domain on the checks and balances that exist within each of them. The Panel hope this process will continue, and that further thought will be given in particular to the need to keep the public informed. We do not believe there is a reason why GCHQ's Ethical Framework or Policy on Whistleblowing could not be made public, for example.

5.62 While the existence of checks and balances within the system is positive, these have not been sufficiently shared with the wider public. There are significant improvements to be made to the external mechanisms in place to oversee the activities of the agencies and hold them to account. It is important not only that oversight is carried out, but that it is *seen* to be done effectively by the general public. While the SIAs have taken recent positive steps to enhance public confidence, overall public recognition and understanding of mechanisms such as the IPT and commissioners is currently poor.

5.63 While the IPT serves an important function, the Panel note that the Tribunal has been seen as opaque and inaccessible to the wider public. Not all hearings or, more importantly, rulings are made public (though we accept there may be good reason for hearings to be confidential in some circumstances). The only avenue of appeal to a ruling by the IPT is via the European Court of Human Rights.

5.64 The commissioners do not have a significant public profile. Despite providing substantial oversight of warrants and the activities of the agencies, the work of the commissioners does not currently translate into greater levels of public understanding. Their annual reports place a great deal of information in the public domain on the work of the agencies and their compliance with legal regulations, but these are not widely read or publicly debated.

5.65 There is a lack of understanding (even internally) of the division of roles and responsibilities between each commissioner. The confusing cartography of commissioners, a consequence of their roles developing in a piecemeal manner, does little to reassure the public of the rigorous oversight of intelligence and law-enforcement agencies. Many of their responsibilities are currently carried out on a non-statutory basis.

5.66 The offices of some of the commissioners are very proficient (especially IOCCO). It is important to ensure that all commissioners are supported by sufficient resources to ensure the breadth and depth of investigations. These resources should comprise a breadth of expertise (to be able to consider broad, thematic issues), a depth of knowledge in certain areas (including technical knowledge of coding and algorithms to inspect

methods of data collection and analysis, for example) and individuals from a variety of backgrounds (including those with technical, legal, investigative and NGO experience).

Investigatory Powers Tribunal

Recommendation 11: The Investigatory Powers Tribunal (IPT) should be as open as possible and proactively find ways that make its business less opaque to the public.

Recommendation 12: The IPT should hold open public hearings, except where the Tribunal is satisfied that private or closed proceedings are necessary in the interests of justice or other identifiable public interest.

Recommendation 13: The IPT should have the ability to test secret evidence put before it by the SIAs. While internal procedures are a matter for the Tribunal to decide, we suggest that this could be achieved through the appointment of a special counsel.

Recommendation 14: We agree with both the ISC and Anderson reports that the domestic right of appeal is important and should be considered in future legislation.

Recommendation 15: Appointment to the IPT should be limited to a term of four years, renewable once for a further four years.

Recommendation 16: The judicial commissioners should have a statutory right to refer cases to the IPT where they find a material error or arguable illegality or disproportionate conduct.

A National Intelligence and Surveillance Office

Recommendation 17: The Intelligence Services Commissioner, Interception of Communications Commissioner's Office, and the Office of Surveillance Commissioners should be replaced by a new single independent organisation: a National Intelligence and Surveillance Office (NISO). This organisation should be placed on a statutory footing and its independence guaranteed by statute.

Recommendation 18: A NISO should have an office based outside of the Whitehall departments, have a public profile and be led by a senior public official. The new organisation should be staffed by appropriate persons with technical, legal, investigative and other relevant expertise (for instance in privacy and civil liberties). The new organisation would have four main areas of responsibility:

- Inspection and audit
- Intelligence oversight
- Legal advice
- Public engagement.

Recommendation 19: A NISO should provide support and assistance to the Investigatory Powers Tribunal and the judicial commissioners.

Collaboration between the Public and Private Sectors

5.67 This Review is primarily concerned with the relationship between the government's use of data and the rights of the public. Nevertheless, as we have sought to demonstrate, the private sector (and CSPs in particular) is a crucial part of the picture, and the relationship between the public and private sectors is a key element in the grand bargain we outline above. It is beyond the scope and the research of our inquiry to make recommendations for the private sector directly, but we have treated it in this Review as essential context to our understanding of the problem and our suggestions for improvements to the current situation.

5.68 The private sector is highly internationalised and evolves rapidly, yet its role tends to be overlooked in debates over privacy and security. Given that commercial organisations are the largest generators and guardians of citizens' data, it is important to understand the types and volumes of data collected and what is subsequently done with it. The collection and manipulation of bulk data is not something unique to government, but rather a pervasive technique which a growing number of organisations, both in the private as well as the public sector, now use to interact with the public as citizens and customers.

5.69 In recognising its importance in debates over privacy and intrusion, we note certain features in the relationship between government and the private sector. One is that levels of co-operation between government agencies and Internet companies are variable. In the immediate wake of the Snowden disclosures, many of the large US companies actively distanced themselves from governments to reassure their customers that they were not complicit in the allegations being made.

5.70 Two years on from the original disclosures, however, the picture is more nuanced. From our visits and evidence sessions, the Panel are confident that good working relationships still exist in the UK at the operational level between CSPs and the law-enforcement agencies and SIAs. This is inevitably so where CSPs have infrastructure located in this country, over and above their provision of services within the UK. The main challenge that law-enforcement, security and intelligence officers now face is that they must establish working relations for the potential provision of data with a growing number of other providers – such as mobile virtual network operators which provide services on another company's wireless network, and many other new types of communications providers – particularly those based overseas.

5.71 At the strategic and policy level, the Panel note that co-operation between the government and CSPs is more disjointed. From our evidence sessions, we understand that some of the biggest Internet companies see themselves as fundamentally global enterprises and interpret their relations with all governments around the world through

that lens. On the other hand, some of the most innovative companies, though not always the biggest, have recently entered into active dialogue with the US government to explore better ways of restoring levels of co-operation that meet all their needs. The US president's National Security Telecommunications Advisory Committee has worked to build new bridges between the US government and industry in the last two years, and the president's Cybersecurity and Consumer Protection Summit in February 2015 was another step in the direction of better relations – all of which matters greatly to UK authorities since many of the companies most relevant to them are based in the US.[18]

5.72 The UK has its own Telecommunications Industry Security Advisory Council, which brings government and the CEOs of the telecoms industry together, and its work will assume greater importance in view of the challenges identified by this report.

5.73 In September 2014, Sir Nigel Sheinwald was appointed 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'.[19] 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.[20]

5.74 Efforts to bridge the current gap between the government and the major Internet companies are certainly welcome but will have to go much further, on both sides, if Internet governance is to be progressed. As the Global Commission on Internet Governance makes clear in its recent findings, it is now 'essential that governments, collaborating with all other stakeholders, take steps to build confidence that the right to privacy of all people is respected on the Internet [and] at the same time to ensure the rule of law is upheld'.[21]

The International Context

5.75 There are very good reasons why the UK's intelligence agencies share information with partner agencies in other countries. However, there is a reasonable expectation from

18. Barack Obama, 'Remarks by the President at the Cybersecurity and Consumer Protection Summit', Stanford University, 13 February 2015.
19. Cabinet Office, 'Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing – Sir Nigel Sheinwald', 2015, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/438326/Special_Envoy_work_summary_final_for_CO_website.pdf>.
20. *Ibid.*
21. Global Commission on Internet Governance, 'Towards a Social Compact for Digital Privacy and Security', CIGI/Chatham House, 2015.

the public that this data-sharing will be done in accordance with UK law. Currently, there is insufficient clarity over the powers and safeguards governing the exchange of data and intelligence between international partners.

5.76 By its nature, the Internet crosses the national jurisdictions which confine national governments, law-enforcement agencies and the SIAs. For commercial organisations, it is their responsibility to comply with the range of legal frameworks of countries within which they operate, including compliance with requests for data; after all, it is their decision to operate in those countries in the first place.

5.77 For law-enforcement agencies and prosecutors, detecting and responding to crimes and threats to national security online requires a greater level of interstate co-operation. Evidence to the Panel suggests, however, that current legal-assistance processes are burdensome and, crucially, slow in comparison to the pace at which online threats can develop. Effort must be put into improving the efficiency of multi-jurisdictional legal assistance, obliging agencies and prosecutors to provide assistance including, where necessary, obtaining information from CSPs and other commercial organisations based within their jurisdiction.

Mutual Legal Assistance Treaties

Recommendation 20: Urgent improvements are necessary in order to expedite the mutual legal assistance treaty (MLAT) process and, in particular, to the UK–US process in managing data requests. We support the practical reforms suggested by Sir Nigel Sheinwald to the existing MLAT between the UK and the US, to include the greater standardisation of processes, training and improved guidance. The scope for a new and wider international framework between like-minded democratic countries should also be seriously investigated 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.

Annex A. Panel Biographies

Professor Michael Clarke (Chairman)

Michael Clarke is Director General of the Royal United Services Institute.

Professor Heather Brooke

Heather Brooke is an investigative journalist and Professor of Journalism at City University, London. Heather worked as a political and crime reporter in the US before moving to Britain where she specialised in using the Freedom of Information Act, notably winning a High Court case against Parliament for the disclosure of MPs' expenses. She is a Trustee of Privacy International and an Advisory Board Member of the Open Rights Group.

Mrs Lesley Cowley OBE

Lesley Cowley was appointed non-executive Chair of the Driver and Vehicle Licensing Agency in October 2014. She is also a non-Executive Director of (aql) and CERT-UK. She is a former Chief Executive of Nominet, the .uk domain-name registry.

Lord Evans of Weardale KCB DL

Jonathan Evans is a former Director General of the Security Service (MI5). He was appointed as an independent crossbench peer in the House of Lords in December 2014 and is a non-executive Director of HSBC. He is also a Senior Associate Fellow of RUSI.

Baroness Lane Fox of Soho CBE

Martha Lane Fox founded and chairs Go ON UK, a cross-sector digital-skills alliance. She chairs MakieLab and Lucky Voice. In 1998 she co founded lastminute.com. She joined the House of Lords as an independent crossbench peer in March 2013, and was appointed Chancellor of the Open University in March 2014. Martha was the British government's Digital Champion from 2009 to 2013.

Professor John Grieve CBE QPM

A career police officer, former National Coordinator for Counter Terrorist Investigations and Director of Intelligence for the Metropolitan Police, John Grieve is now Professor Emeritus at London Metropolitan University and Director of its Centre for Policing and Community Safety, and a Senior Research Fellow at the University of Portsmouth. From

2004 to 2011 he was a Commissioner for the Independent Monitoring of some aspects of the peace process in Northern Ireland.

Professor Dame Wendy Hall DBE FRS FREng

Wendy Hall is Professor of Computer Science and Executive Director of the Web Science Institute at the University of Southampton, where she was previously the Dean of the Faculty of Physical Sciences and Engineering. She is currently a member of the Global Commission on Internet Governance and a member of the World Economic Forum's Global Advisory Council on Artificial Intelligence and Robotics.

Professor Lord Hennessy of Nympsfield FBA

Peter Hennessy is a historian and academic specialising in the history of government. Since 1992, he has been Attlee Professor of Contemporary British History at Queen Mary University of London and a Fellow of the British Academy. In 2010 he was appointed as an independent crossbench peer and sits in the House of Lords.

Professor Sir David Omand GCB

David Omand is a former UK Security and Intelligence co-ordinator, Permanent Secretary in the Home Office, Director of GCHQ and Deputy Under Secretary of State for Policy in the Ministry of Defence. He served for seven years on the Joint Intelligence Committee. He is currently a Visiting Professor in the Department of War Studies at King's College London.

Baroness O'Neill of Bengarve CH CBE FBA FRS

Onora O'Neill is an Emeritus Professor of Philosophy at the University of Cambridge, and Chair of the Equalities and Human Rights Commission. She was created a life peer in 1999 and sits as an independent crossbench peer in the House of Lords.

The Rt Hon the Lord Rooker

Jeffrey Rooker is a Labour politician who served as an MP for Birmingham Perry Barr for twenty-seven years, before joining the House of Lords in June 2001. His ministerial appointments included as Home Office Minister for Asylum and Immigration, and Minister of State in the Department for Environment, Food and Rural Affairs. He has served on the Public Accounts Committee and is a former Chairman of the Foods Standards Agency.

Sir John Scarlett KCMG OBE

John Scarlett is a former Chief of the Secret Intelligence Service and a former Chairman of the Joint Intelligence Committee. He is currently Senior Advisor at Morgan Stanley, Chairman of the Strategy Advisory Council at Statoil and an advisor to Swiss Re. He is

Chairman of the Bletchley Park Trust, a Trustee of the Imperial War Museum and a Senior Associate Fellow of RUSI.

Professor Ian Walden

Ian Walden is Professor of Information and Communications Law in the Centre for Commercial Law Studies, Queen Mary University of London. He is a solicitor and Of Counsel to Baker and McKenzie. Ian has previously been involved in law-reform projects including for the World Bank, Council of Europe and the European Commission.

RUSI Secretariat

The ISR Panel would like to thank Charlie Edwards, Calum Jeffray and Lara Medawar who provided assistance with drafting, organisation and administration.

Annex B. Oral Evidence, Visits and Written Submissions

23 October 2014

Round-table with Richard Salgado (Director, Law Enforcement and Information Security, Google) and Verity Harding (UK Public Policy Manager, Google).

21 November 2014

Privacy and technology round-table with Caspar Bowden, Gabrielle Guillemin (Legal Officer, Article 19), Glyn Moody and Andrew Puddephatt (Executive Director, Global Partners Digital).

1 December 2014

Visit to GCHQ with Robert Hannigan (Director), and staff.

11 December 2014

Round-table with Jane Horvath (Global Head of Privacy, Apple), Gary Davis (Head of Privacy (Europe), Apple) and Claire Thwaites (Senior Director, Government Affairs (EMEIA), Apple).

16 January 2015

Workshop with Giles Herdale (Head of Digital Intelligence and Investigation, the College of Policing).

26 January 2015

Screening of *Citizenfour* and discussion with Emma Carr (Director, Big Brother Watch), Jim Killock (Executive Director, Open Rights Group) and Eric King (Deputy Director, Privacy International).

10 February 2015

Round-table with representatives of the Reform Government Surveillance initiative: Emma Ascroft (Director, Public Policy, Yahoo), Verity Harding (UK Public Policy Manager, Google), Nick Pickles (UK Public Policy Manager, Twitter) and Rishi Saha (Head of Public Policy, Facebook).

19 February 2015

Workshop on latest public opinion trends on privacy and government policy with Gideon Skinner (Director of Political Research, Ipsos MORI).

24 February 2015

Roundtable with: Christopher Graham (Information Commissioner), Sir Mark Waller (Intelligence Services Commissioner), Joanna Cavan (Head of IOCCO, on behalf of Sir Anthony May, Interception of Communications Commissioner), Tony Porter (Surveillance Camera Commissioner) and Clare Ringshaw-Dowle (Chief Surveillance Inspector, on behalf of Sir Christopher Rose, Chief Surveillance Commissioner).

4 March 2015

Visit to the Security Service with Andrew Parker (Director General) and staff.

17 March 2015

Roundtable with TechUK members Stuart Aston (Chief Security Officer, Microsoft), Andy Bates and David Daems (Verizon), Martin Beauchamp (BT), John Davies (Director, Strategy and Government Relations, BAE Systems Applied Intelligence), Ruth Davis (Head of Programme, Cyber, Justice and National Security, TechUK), and Talal Rajab (Programme Manager – Cyber, Justice, and National Security, TechUK).

19 March 2015

Visit to the Foreign and Commonwealth Office.

24 March 2015

Visit to the National Crime Agency with Keith Bristow (Director General) and staff.

31 March 2015

Round-table with Michael Drury (BCL Burton Copeland), Nicholas Griffin QC (5 Paper Buildings) and Ben Jaffey (Blackstone Chambers).

13 April 2015

Conversation with James Ball, Special Projects Editor, *The Guardian*.

20 April 2015

Visit to the Metropolitan Police with Assistant Commissioner Mark Rowley and staff.

1 May 2015

Visit to the Secret Intelligence Service with Alex Younger (Chief) and staff.

Evidence Submissions

Big Brother Watch

Christopher Graham, Information Commissioner's Office

Crown Prosecution Service

Dr Victoria Wang, Institute of Criminal Justice Studies, University of Portsmouth

Professor John Tucker, Department of Computer Science, Swansea University

Other Contacts and Meetings

Ben Wisner (Director, Speech, Privacy and Technology Project, American Civil Liberties Union)

Bibliography

AOL et al., 'Reform Government Surveillance: The Principles', 2014, <https://www.reformgovernmentsurveillance.com/>.

Apple, 'A Message from Tim Cook about Apple's Commitment to Your Privacy', <https://www.apple.com/uk/privacy/>, accessed 10 June 2015.

Anderson, David, *A Question of Trust: Report of the Investigatory Powers Review (Anderson Report)* (London: The Stationery Office, 2015).

Bartlett, Jamie and Krasodomski-Jones, Alex, 'Online Anonymity: Islamic State and Surveillance', Demos, 2015.

Bartlett, Jamie, 'What Does the Dark Net Mean for the Future of Intelligence Work?', speech given at the 2014 Annual Vincent Briscoe Security Lecture, Imperial College, London, 29 October 2014.

Big Brother Watch, 'A Legacy of Suspicion: How RIPA Has Been Used by Local Authorities and Public Bodies', 2012.

Big Brother Watch, 'Police Access to Communications Data: How UK Police Forces Requested Access to Communications Data over 700,000 Times in 3 Years', 2015.

Big Brother Watch, 'Response to the Intelligence and Security Committee Report on Privacy v Security', media release, 12 March 2015, <https://www.bigbrotherwatch.org.uk/media-and-press/response-to-the-intelligence-and-security-committee-report-on-privacy-v-security/>, accessed 11 June 2015.

Big Brother Watch, 'The Grim RIPA: Cataloguing the Ways in Which Local Authorities Have Abused Their Covert Surveillance Powers', 2010.

Big Brother Watch, 'UK Public Research – Online Privacy', 2015.

Blears, Hazel, letter to Renate Samson, Chief Executive of Big Brother Watch, 17 March 2015, <http://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/03/20150317-ISC-421-146-ISC-to-Renate-Samson-BBW.pdf>.

Bowden, Casper, 'Privacy and Security Inquiry: Submission to the Intelligence and Security Committee of Parliament', 2014.

Bowden, Casper, 'Submission to the Joint Committee on the Draft Communications Data Bill', 2012.

Brown, Ian, 'Witness Statement of Dr Ian Brown', statement to the European Court of Human Rights, Application No. 58170/13, 27 September 2013.

Cabinet Office, 'National Intelligence Machinery', 2010.

Cabinet Office, 'Supporting the National Security Council (NSC): the Central National Security and Intelligence Machinery', 2011.

Cameron, David, 'Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015', 11 March 2015.

Carr et al., uncorrected submission of evidence to the ISC Privacy and Security Inquiry, Public Evidence Session 2, 15 October 2014.

Centre for International Governance Innovation and Ipsos, 'CIGI-Ipsos Global Survey on Internet Security and Trust', 2014.

Edwards, Charlie and Fieschi, Catherine (eds), *UK Confidential* (London: Demos, 2008).

Graham, Christopher, *Information Commissioner's Annual Report and Financial Statements 2013/14: Effective, Efficient – and Busier Than Ever* (London: The Stationery Office, 2014).

Clegg, Nick, uncorrected submission of evidence to the ISC Privacy and Security Inquiry, Public Evidence Session 6, 15 October 2014.

Committee on Civil Liberties, Justice and Home Affairs, 'Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs', European Parliament, A7-0139/2014, 2014.

Council of Europe, Commissioner for Human Rights, 'Democratic and Effective Oversight of National Security Services', Issue Paper, Council of Europe, 2015.

Kaye, David, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', UN Human Rights Council, A/HRC/29/32, 22 May 2015.

Don't Spy on Us, 'Don't Spy on Us: Reforming Surveillance in the UK', 2014.

Economist, 'A Tangled Web: Who Goes Online, and Where', 8 November 2014.

Economist, 'Data, Data Everywhere', 25 February 2010.

Economist, 'Drawing the Line', 4 October 2014.

Economist, 'Little Brother', 13 September 2014.

Economist, 'The Spy in Your Pocket', 28 February 2015.

Economist, 'The Truly Personal Computer', 28 February 2015.

Economist, 'The World Wild Web', 13 September 2014.

Economist, 'What's Up?', 25 March 2015.

Economist, 'Not-So-Private Lives', 4 April 2015.

Economist, 'Reviewing the Surveillance State: America', 23 May 2015.

Enserink, Martin and Chin, Gilbert, 'The End of Privacy', *Science* (Vol. 347, No. 6221, January 2015), pp. 490–91.

European Commission, Justice, 'Collecting and Processing Personal Data: What Is Legal?', 2015, <http://ec.europa.eu/justice/data-protection/data-collection/legal/index_en.htm>.

Evans, Jonathan, 'Maiden Speech', *Hansard*, Lords Hansard, Col. 690 (13 January 2015).

Farr, Charles, 'Witness Statement of Charles Blandford Farr on Behalf of the Respondents', evidence submitted to the Investigatory Powers Tribunal, 16 May 2014.

Federal Trade Commission, 'Internet of Things: Privacy and Security in a Connected World', Staff Report, 2015.

Global Commission on Internet Governance, 'Towards a Social Compact for Digital Privacy and Security', CIGI/Chatham House, 2015.

Hansard, House of Commons Debates, 'Anderson Report', Col. 1353–68 (11 June 2015).

HM Government, 'Emerging Technologies: Big Data', Horizon Scanning Programme, December 2014.

HM Government, Secretary of State for the Home Department, 'Draft Communications Data Bill', June 2012.

Home Office, 'Data Retention Legislation – Privacy Impact Assessment', 2014.

Home Office, 'Regulation of Investigatory Powers Act 2000: Consultation: Equipment Interference and Interception of Communications Codes of Practice', 2015.

Home Office, 'Retention of Communications Data: Code of Practice', draft for public consultation, 2015.

Home Office, *Acquisition and Disclosure of Communications Data: Code of Practice* (London: The Stationery Office, 2015).

Home Office, 'Equipment Interference: Code of Practice', draft for public consultation, 2015.

Home Office, *Interception of Communications: Code of Practice* (London: The Stationery Office, 2007).

Home Office, 'Regulation of Investigatory Powers Act 2000, Consultation: Equipment Interference and Interception of Communications Codes of Practice', 6 February 2015.

House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State. Vol 1: Report* (London: The Stationery Office, 2009).

House of Lords, House of Commons, Joint Committee on the Draft Communications Data Bill, 'Draft Communications Data Bill', Session 2012–13, HC 479, 2012.

House of Lords, Select Committee on Digital Skills, 'Make or Break: The UK's Digital Future', Report of Session 2014–15, HL Paper 111, 2015.

Information Commissioner's Office (ICO) et al., 'Surveillance Road Map: A Shared Approach to the Regulation of Surveillance in the United Kingdom', Version 3.3, 2015.

Information Commissioner's Office, 'Annual Track 2014: Individuals (Topline Findings)', 2014.

Information Commissioner's Office, 'Protecting Personal Data in Online Services: Learning from the Mistakes of Others', Version 1, 2014.

Intelligence and Security Committee of Parliament (ISC), 'Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme', 2013.

Intelligence and Security Committee of Parliament, *Access to Communications Data by the Intelligence and Security Agencies* (London: The Stationery Office, 2013).

Intelligence and Security Committee of Parliament, *Annual Report 2013–2014* (London: The Stationery Office, 2014).

Intelligence and Security Committee of Parliament, *Privacy and Security: A Modern and Transparent Legal Framework* (London: The Stationery Office, 2015).

Intelligence and Security Committee of Parliament, *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby* (London: Stationery Office, 2014).

Interception of Communications Commissioner's Office, 'Evidence for the Investigatory Powers Review', 2014.

Investigatory Powers Tribunal, 'Approved Judgment', Liberty & Others vs. the Security Service, SIS, GCHQ IPT/13/77/H, 5 December 2014.

Investigatory Powers Tribunal, 'Approved Judgment', Liberty & Others vs. the Security Service, SIS, GCHQ IPT/13/77/H, 6 February 2015.

Ipsos MORI, 'Privacy and Personal Data: Poll Conducted by Ipsos MORI for the Joseph Rowntree Reform Trust', Joseph Rowntree Reform Trust, 2014.

Ipsos MORI, 'Understanding Society: The Power and Perils of Data', 2014.

Johnson, Loch K et al., 'An *INS* Special Forum: Implications of the Snowden Leaks', *Intelligence and National Security* (Vol. 29, No. 6, August 2014).

Kennedy, Paul, *2012 Annual Report of the Interception of Communications Commissioner* (London: The Stationery Office, 2013).

Kent, Gail, 'The Mutual Legal Assistance Problem Explained', The Center for Internet and Society, February 2015, <http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained>.

Libe Committee Inquiry on US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs, 'List of Hearings and Experts', 2013.

Lobban, Iain, 'Valedictory Speech', speech given at the Cabinet War Rooms, London, 21 October 2014.

Martha Lane Fox, speech delivered at the 2015 Richard Dimbleby Lecture, 30 March 2015.

May, Anthony, *2013 Annual Report of the Interception of Communications Commissioner* (London: The Stationery Office, 2014).

May, Anthony, *Report of the Interception of Communications Commissioner: March 2015* (London: The Stationery Office, 2015).

Microsoft, 'Data Privacy Day 2013 Survey Results', January 2013.

Moore, Martin, 'RIP RIPA? Snowden, Surveillance, and the Inadequacies of Our Existing Legal Framework', *The Political Quarterly* (Vol. 85, No. 2, April/June 2014).

Newman, Abraham L, 'What the "Right to Be Forgotten" Means for Privacy in a Digital Age", *Science* (Vol. 347, No. 6221, January 2015), pp. 507–08.

Ofcom, 'Half of UK Homes Turn to Tablets – in Just Five Years', news release, 27 May 2015, <http://media.ofcom.org.uk/news/2015/five-years-of-tablets/>.

Ofcom, 'Promoting Investment and Innovation in the Internet of Things: Summary of Responses and Next Steps', Statement, 2015.

Omand, David, 'Understanding Digital Intelligence and the Norms That Might Govern It', Global Commission on Internet Governance, Paper Series, No. 8, CIGI/ Chatham House, 2015.

Omand, David, uncorrected submission of evidence to the ISC Privacy and Security Inquiry, Public Evidence Session 8, 23 October 2014.

Parliamentary Office of Science and Technology, 'Big Data: An Overview', Postnote, No. 468, 2014.

Parliamentary Office of Science and Technology, 'Monitoring Internet Communications', Postnote, No. 436, 2013

Parliamentary Office of Science and Technology, 'Social Media and Big Data', Postnote, No. 460, 2014.

Parliamentary Office of Science and Technology, 'The Darknet and Online Anonymity', Postnote, No. 488, 2015.

Perri 6, *Future of Privacy. Vol 1* (London: Demos, 1998).

Perri 6, Kristen Lasky and Adrian Fletcher, *Future of Privacy. Vol. 2* (London: Demos, 1998).

The President's Review Group on Intelligence and Communications Technologies, 'Liberty and Security in a Changing World', 2013.

Richards, Martin, 'Let Public Have Greater Say over Big Health Data', *New Scientist*, 3 February 2015.

Robbins, Oliver, 'First Witness Statement of Oliver Robbins', statement to the High Court, CO/11732, 27 August 2013.

Rusbridger, Alan, speech given at RUSI, London, 19 January 2015.

Salgado, Richard, 'Written Testimony of Richard Salgado, Director, Law Enforcement and Information Security, Google, Inc.', Senate Judiciary Subcommittee on Privacy, Technology and the Law, Hearing on 'The Surveillance Transparency Act of 2013', 13 November 2013.

Samson, Renate, letter to Michael Gibson, Senior Assistant Clerk to the Committee, Intelligence and Security Committee, 13 March 2015, <http://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/03/Big-Brother-Watch-letter-to-ISC-13th-March-2015.pdf>.

Sawers, John, Lobban, Iain and Parker, Andrew, uncorrected submission of evidence to the ISC Privacy and Security Inquiry, Public Evidence Session, 7 November 2013.

ScienceWise, 'Big Data: Public Views on the Collection, Sharing and Use of Personal Data by Government and Companies', 2014.

Statutory Instruments, 'The Regulation of Investigatory Powers (Communications Data) Order 2010', No. 480.

Statutory Instruments, 'The Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2015', No. 228.

Stiglitz, Joseph E, 'On Liberty, the Right to Know, and Public Discourse: The Role of Transparency in Public Life', Oxford Amnesty Lecture, 1999.

Stratford, Jemima, and Johnston, Tim, 'In the Matter of State Surveillance', advice to Tom Watson MP, 22 January 2014.

TRUSTe, 'TRUSTe Privacy Index', 2014 UK Consumer Data Privacy Study, <https://www.truste.com/resources/privacy-research/uk-consumer-confidence-index-2014/>.

Vodafone, 'Vodafone's Written Evidence to the Investigatory Powers Review', news release, 24 October 2014, <http://www.vodafone.com/content/index/about/about-us/privacy/uk-investigatory-power.html>, accessed 12 June 2015.

White House, 'Big Data: Seizing Opportunities, Preserving Values', Interim Progress Report, February 2015.

Wittes, Benjamin and Liu, Jodie C, 'The Privacy Paradox: The Privacy Benefits of Privacy Threats', Center for Technology Innovation, Brookings Institute, 2015.

Wood, David Murakami (ed.), 'A Report on the Surveillance Society: For the Information Commissioner by the Surveillance Studies Network', 2006.

World Wide Web Foundation, 'Open Data Barometer Global Report', 2nd edition, 2015.

Legislation

Anti-terrorism, Crime and Security Act 2001

Computer Misuse Act 1990

Data Protection Act 1998

Data Retention and Investigatory Powers Bill, Draft Bill

Data Retention (EC Directive) Regulations 2009

Intelligence Services Act 1994

Justice and Security Act 2013

Protection of Freedoms Act 2012

Security Service Act 1989

Wireless Telegraphy Act 2006

A Democratic Licence to Operate: Report of the Independent Surveillance Review
Whitehall Report 2-15

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)