Operational Case for Bulk Powers

Contents

1. Introduction

Background

1.1. In November 2015, the Government published the draft Investigatory Powers Bill, responding to the recommendations of three independent reviews undertaken by the Intelligence and Security Committee of Parliament; David Anderson QC, the Independent Reviewer of Terrorism Legislation; and a panel convened by the Royal United Services Institute (RUSI).

1.2. Those reviews made nearly 200 recommendations for reform of the law governing investigatory powers. The draft Investigatory Powers Bill brought together those powers already available to the security and intelligence agencies to obtain communications and data about communications. It seeks to update the law to reflect technological change, ensuring that these powers – including those relating to sensitive capabilities available to the security and intelligence agencies – are set out transparently and consistently, with robust safeguards and world leading oversight.

1.3. The draft Bill was subject to pre-legislative scrutiny by three Parliamentary Committees: the House of Commons Science and Technology Committee, the Intelligence and Security Committee and a Joint Committee convened to scrutinise the draft Bill.

1.4. The Joint Committee recommended that the Government should publish a fuller justification for each of the bulk powers alongside the Bill (recommendations 23 and 28). This document responds to those recommendations. It should be read alongside the revised Bill introduced on 1 March, the Government's response to each of the Parliamentary Committees that scrutinised the draft Bill, and the six detailed Codes of Practice published in draft alongside the Bill on introduction.

Bulk powers

1.5. The security and intelligence agencies – the Security Service (MI5), Government Communications Headquarters (GCHQ), and the Secret Intelligence Service (SIS) – exist to defend the UK's national security and to protect its citizens. The threats to the UK are diverse and constantly evolving. They include terrorism, serious crime, the resurgence of state-based threats and cyber-attacks. As the 2015 National Security Strategy made clear, the security and intelligence agencies are increasingly likely to have to deal with unexpected threats and risks to our security.

1.6. Meanwhile, in parallel, technological changes have transformed the challenge facing the security and intelligence agencies. Terrorists and criminals have embraced modern communication networks to plan, coordinate and increasingly to execute their attacks. The growth of the internet and encryption has steadily reduced the ability of conventional and targeted intelligence approaches alone to tackle these challenges.

1.7. Bulk powers have been essential to the security and intelligence agencies over the last decade and will be increasingly important in the future. The acquisition and use of bulk data – information acquired in large volumes and used subject to special restrictions – provides vital and unique intelligence that the security and intelligence agencies cannot obtain by any other means. The security and intelligence agencies use the same techniques that modern businesses increasingly rely on to analyse data in order to overcome the most significant national security challenges. They do so subject to strict safeguards and robust oversight.

Bulk capabilities are among the most important tools that the agencies can use to:

- obtain intelligence on overseas subjects of interest, including threats to UK citizens and our Armed Forces;
- identify threats here in the UK, sometimes from fragments of intelligence;
- establish and investigate links between known subjects of interest, at pace, in complex investigations;
- understand known suspects' behaviour and communications methods to identify potential attack planning;
- verify information obtained about subjects of interest through other sources (e.g. agents); and
- resolve sometimes anonymous online personae to real world identities.

1.8. There is clear evidence that these capabilities have helped to protect the UK. The analysis of bulk data, for example, has:

- played a significant part in every major counter terrorism investigation of the last decade, including in each of the seven terrorist attack plots disrupted since November 2014;

- enabled over 90% of the UK's targeted military operations during the campaign in the south of Afghanistan;

- been essential to identifying 95% of the cyber-attacks on people and businesses in the UK discovered by the security and intelligence agencies over the last six months; and

- been used to identify serious criminals seeking to evade detection online, and who cannot be pursued by conventional means, supporting the disruption of over 50 paedophiles in the UK in the last three years.

1.9. This document sets out the case for these powers in more detail. It explains:

- how bulk powers are used by the security and intelligence agencies today and why they are so valuable to our security;

- why trends in technology and the current threat environment mean that the use of bulk powers will be a vital tool for identifying and investigating threats in the future; and

- what the Investigatory Powers Bill will do to put those existing powers on a clearer statutory footing with robust safeguards and world-leading oversight.

1.10. It includes a series of examples and case studies to illustrate the value of those powers. There are necessarily limits on the level of detail that can be provided in public without handing an advantage to those who mean us harm. For that reason, the security and intelligence agencies have made available to the Intelligence and Security Committee of Parliament further classified information about the examples used.

2. What are bulk powers?

2.1. The security and intelligence agencies use a range of techniques under existing legislation to acquire information in large volumes. This information, sometimes referred to as 'bulk data', is used by the security and intelligence agencies to generate intelligence about threats that cannot be acquired by more targeted means.

2.2. The law today allows the security and intelligence agencies to acquire bulk data in four ways:

- Through the **bulk interception of communications**. This involves intercepting international communications as they travel across networks. It is often one of the only ways of obtaining intelligence on threats emanating from overseas, frequently in places where the UK Government has a very limited presence.

- Through **bulk equipment interference**. This involves the acquisition of communications and equipment data directly from computer equipment overseas. Historically, this data may have been available during its transmission through bulk interception. The growing use of encryption has made this more difficult and, in some cases, equipment interference may be the only option for obtaining crucial intelligence. As with bulk interception this is an overseas collection capability.

- As **bulk communications data**, obtained from communications service providers. Communications data can be invaluable in identifying the links between subjects of interest and uncovering networks. The law provides for the acquisition of communications data relating to people in the UK and overseas.

- As **bulk personal datasets**. This involves the use of datasets such as travel data or Government databases. Like communications data, the information included in those datasets is generally less intrusive than data acquired through equipment interference or interception. The law provides for the obtaining of bulk personal datasets relating to people in the UK and overseas.

2.3. The security and intelligence agencies have never collected data indiscriminately, and they operate in accordance with strict safeguards, under the oversight of the Interception of Communications Commissioner, the Intelligence Service Commissioner, and the Intelligence and Security Committee of Parliament. The Investigatory Powers Bill will further strengthen the safeguards, introducing a new 'double-lock', so that bulk warrants authorised by the Secretary of State must also be approved by a Judicial Commissioner. Those warrants will also specify the more detailed Operational Purposes for which material acquired under those warrants may be examined.

2.4. The security and intelligence agencies have never collected data indiscriminately, and they operate in accordance with strict safeguards, under the oversight of the Interception of Communications Commissioner, the Intelligence Service Commissioner, and the Intelligence and Security Committee of Parliament. The Investigatory Powers Bill will further strengthen the safeguards, introducing a new 'double-lock', so that bulk warrants authorised by the Secretary of State must also be approved by a Judicial Commissioner. Those warrants will also specify the more detailed Operational Purposes for which material acquired under those warrants may be examined.

Why are they needed?

2.5. Subject to stringent safeguards, bulk powers provide vital intelligence that cannot be generated from any other source - conventional targeted techniques are insufficient on their own to deal with the range of threats. In countries such as Syria, where the UK has no physical presence, there are often no initial intelligence leads on emerging threats. Bulk powers allow the security and intelligence agencies to identify and map out known and evolving networks, in turn enabling further intelligence gathering on likely threats. Within the UK itself, the analysis of bulk communications data or bulk personal datasets is often the only way for the security and intelligence agencies to progress investigations and identify terrorists from very limited lead intelligence, or when their communications have been deliberately concealed.

Necessity and proportionality

2.6. Warrants for the use of these powers are only issued where it is both necessary and proportionate to do so. Each warrant must be clearly justified and will balance intrusions into privacy against the expected intelligence benefits.

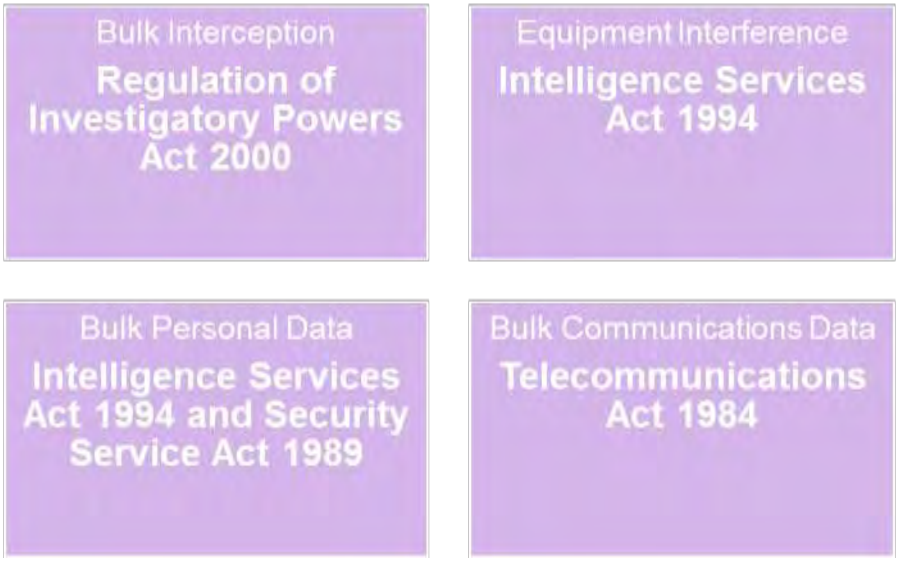
2.7. Strict safeguards limit any access to data obtained under a bulk warrant, so that it is only searched or examined where there is a clear justification. Unnecessary collection or examination of data, such as random or unjustified searches, would be unlawful and may be subject to criminal prosecution. Further guidance on how the necessity and proportionality tests must be applied in practice is provided in the draft Codes of Practice published alongside the Bill.

Foreign-focused powers

2.8. Bulk interception and bulk equipment interference are foreign-focused powers, which allow the security and intelligence agencies to gather overseas-related communications of terrorists, serious criminals and state based threats in parts of the world where the UK may have a limited or no physical presence. Warrants for these powers must not be sought with the intention of acquiring the communications or private data of people in the UK.

Further information

2.9. All of these powers are already available to the security and intelligence agencies under existing legislation. The Government has published Codes of Practice, handling arrangements and other guidance on their use.



Bulk Interception

Regulation of Investigatory Powers Act 2000

Equipment Interference

Intelligence Services Act 1994

Bulk Personal Data

Intelligence Services Act 1994 and Security Service Act 1989

Bulk Communications Data

Telecommunications Act 1984

2.10. This document provides further information about how these powers are used and why they are needed. Chapter 5 provides more detail about how these powers used and why they are so valuable in helping to keep the UK and its citizens safe. Chapter 6 provides further detail on how bulk powers are provided for in the Investigatory Powers Bill. Chapters 7 to 10 provide detail about each of the individual bulk powers.

3. Technological change

Social and economic change

3.1. Our society and economy have been transformed by developments in communications technology. The growth of the internet, mobile telecommunications and computing power - backed by strong encryption and cyber security - have brought huge benefits to UK businesses and citizens. They have enabled on-line commerce, increased international trade and created new business opportunities for the UK's growing IT sector. The advent of social media has presented new ways for people to communicate and live their lives.

3.2. This same technology has also been adopted by terrorists, criminals and others who seek to harm individuals in the UK. The operating environment for the security and intelligence agencies has fundamentally changed: our adversaries are now exploiting the internet, the "dark web" and encryption to remain anonymous and hidden. The security and intelligence agencies have developed analytical techniques using bulk data to mitigate the threat and these will become increasingly important over the coming years.

3.3. The use of 'big data' is an increasingly common feature of the internet economy. Data analytics are used by businesses and governments to navigate substantial volumes of data. These same techniques are used by the security and intelligence agencies to identify patterns of behavior that identify threats to the UK hiding among innocent communications, and to obtain intelligence on overseas targets that could not be acquired by conventional, more targeted means.

Global trends

3.4. Over the last 20 years, the number of internet users has increased exponentially. This has been driven by increased access to mobile communications – allowing people to access the internet outside of the home or workplace – and a much wider range of software applications for users. This has transformed global patterns of behaviour:

- By 2019, 71% of the world's population will have access to a mobile internet device.

- Globally, the average mobile device's data traffic will treble between 2014 and 2019.

- In 2012 the number of online instant messages (19 billion) that were sent overtook the number of conventional text messages (17.6 billion).

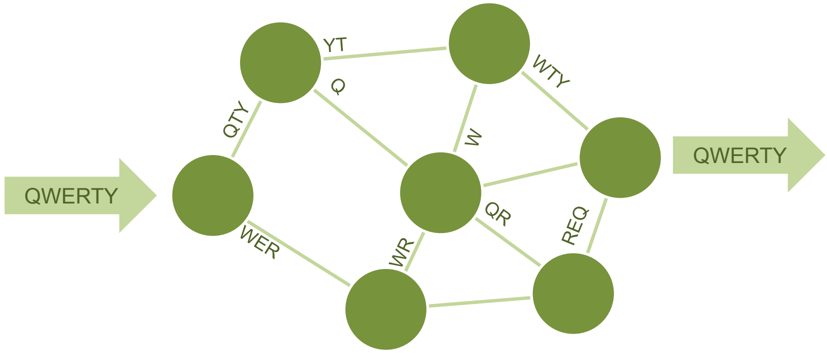
3.5. The benefits to businesses and consumers are considerable. However, the proliferation of new means of communications also affords new opportunities to terrorists and serious criminals. The internet provides alternative means to plan operations and inspire attacks, and the scale of the internet makes it easier for the communications of hostile actors to hide among innocent traffic and reduces the value of targeted techniques.

3.6. Criminals and terrorists will often use multiple devices and applications in a deliberate effort to avoid detection. Analysts can no longer assume that a terrorist or criminal will use a specific phone or application, or that targeted requests to communications service providers will generate a sufficient picture of their activity to enable a prosecution or to prevent an attack from taking place. The security and intelligence agencies have had to work in different ways to understand patterns of behaviour and support investigations. Access to bulk data is an essential part of this response.

How internet communications work

3.7. The nature of internet communications also increases the scale of the challenge for the security and intelligence agencies. There are many possibilities for the route a single internet communication could travel from its origin to its destination. It is split into lots of components ('packets') which transit different routes and are re-assembled at their destination.

Figure 3.1. Internet Communications



3.8. Any response - for example, the webpage a terrorist or serious criminal wants to view - may travel via an entirely different set of routes. This will all be determined in milliseconds at the time of the communication and is hugely unpredictable, even where the sender or recipient of the communication is known.

3.9. To intercept the communications of known targets overseas, the security and intelligence agencies therefore have to intercept communications in bulk in order to increase their chances of obtaining target communications. This will still require them to piece multiple fragments of communications together, meaning the intelligence will still yield an incomplete picture of a suspect's communications.

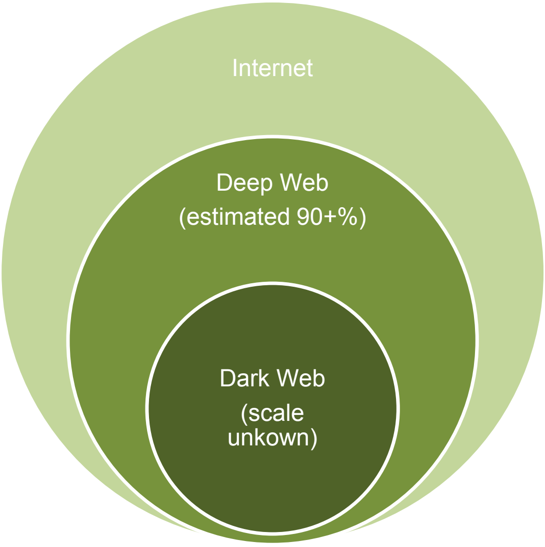
The “dark web”

3.10. The open web is only a small part of the internet. Over 90% of the internet comprises the ‘deep web’: password protected information that is not available to, or searchable by, most internet users. Most of this information is hidden from view for legitimate reasons. However, recent years have witnessed the growth of a new ‘dark web’. Strong encryption and anonymity protocols are intended to ensure the users of these sites cannot be identified.

3.11. The dark web offers users a secure, space in which information can be exchanged anonymously and beyond the reach of law enforcement. These internet services may be hosted in countries without effective legal systems, or be deliberately designed to prevent access by law enforcement agencies.

3.12. There are many valid uses for these internet tools and sites, including by citizens campaigning for civil rights under authoritarian regimes. Terrorists and criminals, however, have also embraced some of these services. These sites and forums provide an anonymous marketplace for those looking to share or obtain sexually explicit images of children or to exchange other criminal services, including illegal firearms, drugs and tools used by cyber criminals.

Figure 3.2. The Dark Web and the Deep Web



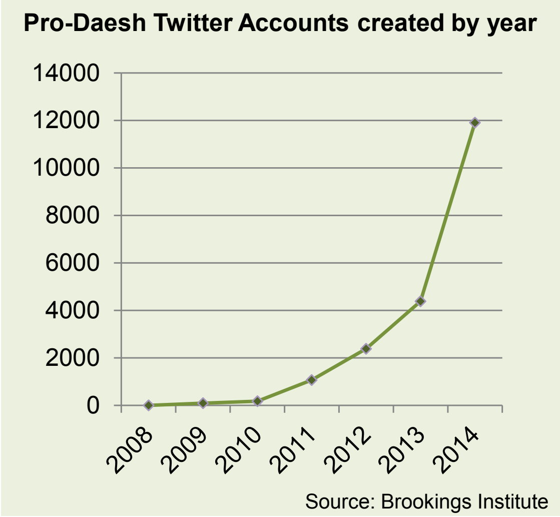
3.13. The use of bulk data is among the few effective methods available to counter the illicit use of the dark web. By analysing data obtained through bulk interception, investigators are able to link the anonymous identities of criminal users to their real world identities. These techniques rely on the analysis of large volumes of data; it would not be possible to do this through targeted interception or communications data powers.

3.14. The security and intelligence agencies have begun to play a vital role in supporting law enforcement to tackle this threat. Bulk data has supported the disruption of over 50 child sexual exploitation offenders in the UK in the last 30 months alone. These capabilities underpin the work of a new Joint Operations Centre between GCHQ and law enforcement to fight child exploitation. The use of bulk data will remain essential for preventing parts of the internet from operating beyond the reach of law enforcement.

Terrorism and social media

3.15. Social media is an important tool for citizens and businesses in the UK. Social media provides new channels of communication and allows people to interact in diverse ways.

3.16. Terrorists and extremist groups in particular have also adopted it as a method of spreading their messages and encouraging attacks against the UK and its allies. Daesh (also known as ISIL) is perhaps the starkest example, using the internet to create a near-global threat and as a means of sending its messages to individuals around the world. Some individuals influenced by this messaging will be vulnerable to radicalisation, potentially turning to violence, sometimes over a very short period of time.


Pro-Daesh Twitter Accounts created by year

Source: Brookings Institute

3.17. Industry and government have worked together to tackle this problem. Twitter, for example, has suspended over 125,000 accounts linked to Daesh in the last eight months alone. The security and intelligence agencies use bulk communications data and bulk personal datasets to gain vital insights into the plans of those plotting against the UK, and to understand the connections between individuals. These capabilities frequently provide one of the only sources of information at the early stages of an investigation. They enable the security and intelligence agencies to respond at pace, moving quickly to identify threats and rule people in or out of investigations. The increasing diversity of terrorist threats, and the speed at which they can escalate through online radicalisation, has made the security and intelligence agencies' bulk capabilities more important.

The challenge of encryption

3.18. Encryption provides a means of making sure communications cannot be read by anyone other than the sender or intended recipient. It is now cheap and almost ubiquitous; strong encryption is typically a default setting in most IT products and on-line services, often without the user ever being aware.

3.19. The spread of encryption has been positive for businesses and citizens. It allows users to live and work on-line, confident that their personal information is secure. The internet economy contributes more to the UK's Gross Domestic Product than that of any other G20 country; this growth has only been possible because of the more widespread use of encryption in commerce and industry. The UK is a world-leader in online security; British companies enjoy rising exports and the UK is seen as a trusted place for online commerce.

3.20. The same technology, however, can be used by terrorists and serious criminals to carry on their activities undetected. The growth in the availability of encrypted communications has had two implications for the security and intelligence agencies. First, they have had to become less reliant on obtaining the content of a suspect's communications: when investigating a known threat in the UK, the agencies will often have to make greater use of bulk data to identify associates and to reveal possible attack planning. Second, the ability to obtain the communications of suspects overseas increasingly requires the use of equipment interference in order to supplement bulk interception.

4. The Threat

4.1. The National Security Risk Assessment 2015 describes the wide range of threats to the UK, including from terrorism, serious crime, cyber-attacks and the resurgence of state-based threats. Terrorists and serious criminals have used the power of the internet and encryption to conceal their operations and to inspire attacks, creating greater challenges for the security and intelligence agencies.

4.2. The nature of the threat has evolved; technology is being used to evade detection and carry out operations in secret. The sheer volume of data means the security and intelligence agencies must constantly develop new techniques and rely upon analysis of bulk data to protect the UK's security. This Chapter outlines the threats to the UK and the role of bulk powers in responding to them.

The threat from Islamist terrorism

4.3. The principal terrorist threat to the UK today is from Islamist terrorism. Daesh has emerged as the most violent of these terrorist groups, threatening UK citizens at home, overseas and online. Daesh has a proven intention and capability to conduct large-scale attacks in Europe. It has exploited modern technology to incite and publicise attacks against the UK and its allies, and to plan ambitious, centrally coordinated operations.

4.4. The threat from Daesh is global. The murder of British hostages in Syria, the attacks on tourists in Tunisia and the terrible events in Copenhagen and Paris have underlined the threat posed to British nationals, and to our allies, around the world. Over 60 British nationals have been killed in overseas terrorist incidents since 2010. The threat level within the UK itself, assessed independently by the Joint Terrorism Analysis Centre, has remained at SEVERE since August 2014, indicating that a terrorist attack is highly likely.

4.5. The security and intelligence agencies have disrupted a succession of plots within the UK, all of which could have resulted in the significant loss of life. Their use of bulk powers are essential to the UK's counter terrorism effort: the analysis of bulk data has played a significant part in every major counter terrorism investigation of the last decade, including in each of the seven UK attack plots disrupted since November 2014.

The threat from Northern Ireland related terrorism

4.6. There is also a continuing threat from Northern Ireland-related terrorism. Dissident republican groupings continue to target the security forces, police and prison officers in Northern Ireland, and continue to aspire to conduct attacks in Great Britain. There were 16 attacks by violent dissident republicans in 2015 that sought to cause harm or death. Countering this threat requires sustained effort from the security and intelligence agencies and the Police Service of Northern Ireland to investigate and disrupt attack planning. Bulk data is essential to these sensitive vital operations.

4.7. For example, analysis of bulk data has been used successfully over many years to identify connections between terrorist groups and to alert the authorities to changes in behaviour that could indicate attack planning.

The threat to military operations

4.8. Our Armed Forces concluded their operations in southern Afghanistan in 2014, after a 13-year campaign to support the stabilisation of the country as part of the NATO-led international mission. British forces faced persistent attacks from the Taleban during the campaign, during which 453 British service personnel lost their lives. The Taleban increasingly adopted secure methods of communication to plan their operations.

4.9. The security and intelligence agencies' bulk powers proved essential for our force protection, enabling the UK to overcome the Taleban's efforts to protect their communications, understand their command and control networks and then predict their attack plans. The security and intelligence agencies' bulk capabilities enabled over 90% of our targeted military operations during the course of the campaign in the south of Afghanistan, helping to save the lives of many UK and Afghan service personnel.

4.10. With the UK playing a leading role in the fight against Daesh in Iraq and Syria, our Armed Forces continue to rely on the intelligence derived from bulk data to identify people overseas who seek to do our troops and the UK harm.

Regional instability and state-based threats

4.11. Regional conflicts and the aggressive behaviour of authoritarian regimes pose an increasing threat to the UK. The conflicts in Syria and Iraq have had an impact on many UK nationals, both at home and in the region. Foreign intelligence agencies have continued to engage in hostile operations against the UK. Bulk capabilities, particularly bulk interception and bulk equipment interference, will be increasingly important to enable the security and intelligence agencies to support our allies around the globe and to protect the UK's national security and economic security by providing an insight into the plans and objectives of hostile governments. Due to the high level and sophistication of communications security used by hostile states, the same intelligence picture could not be provided using targeted powers alone.

Serious crime and child sexual exploitation

4.12. Serious and organised crime affects the lives of everyone in the UK. Serious crime costs the UK at least £24 billion each year and is a growing challenge for both the National Crime Agency (NCA) and the security and intelligence agencies. Of particular concern are those criminals who seek to target the most vulnerable in our society on a massive scale by taking advantage of modern technology and online scams. There are an estimated 50,000 individuals in the UK viewing and sharing child abuse imagery via the internet, for example, supported by a much wider international network.

4.13. The scale of child sexual exploitation around the world, combined with the technical knowledge of the internet demonstrated by many abusers, means that as well as needing to make changes to the law to provide for the retention of internet connection records, bulk capabilities will be increasingly vital to the UK's strategy for protecting children. These capabilities are being deployed through the new Joint Operations Centre, created in 2015 by the NCA and GCHQ to combat child sexual exploitation over the internet.

Cyber security

4.14. The cyber security of the UK is of growing importance to our national security, economy and society. The levels of cyber-attacks by criminals and hostile states have grown considerably; the number of nationally-significant cyber incidents dealt with by the security and intelligence agencies, for example, doubled between 2014 and 2015. Terrorists are increasingly seeking cyber capabilities in order to threaten the critical national infrastructure of the UK. The scale of the challenge is daunting: one recent cybercrime attack alone infected around 150,000 users in the UK.

4.15. The scale of the internet limits the utility of targeted powers and make bulk capabilities critical to the UK's efforts to detect and defend against such attacks. 95% of the cyber-attacks on the UK detected by the security and intelligence agencies over the last six months were only discovered through the collection and analysis of bulk data. These have included numerous attacks against government networks and every major UK commercial sector. The security and intelligence agencies routinely share this unique intelligence with their partners in UK industry, enabling them to protect their businesses and customers from cyber-attacks.

5. How bulk data is used

5.1. The power to acquire and analyse bulk data is crucial to the security and intelligence agencies' effectiveness. Bulk capabilities are used alongside other capabilities to investigate known, high-priority threats and to identify emerging threats from individuals not previously known to the security and intelligence agencies. These capabilities are vital in detecting and disrupting threats to the UK. They are also often the only means to acquire intelligence about overseas and online threats to the UK. This Chapter explains in more detail how the security and intelligence agencies use bulk capabilities to protect the UK.

Access to bulk data is essential to:

- obtain intelligence on overseas subjects of interest, including threats to UK citizens and our Armed Forces;
- identify threats here in the UK, sometimes from fragments of intelligence;
- establish and investigate links between known subjects of interest, at pace, in complex investigations;
- understand suspects' behaviour and communications methods to identify potential attack planning;
- verify information obtained about subjects of interest through other sources (e.g. agents); and
- resolve sometimes anonymous online personae to real world identities.

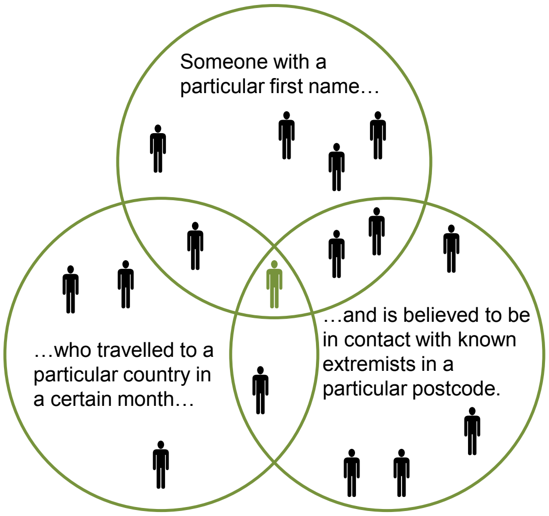
Identifying new threats

5.2. When assessing the significance of a new potential threat to the UK, the security and intelligence agencies will frequently have only small fragments of intelligence or early, unformed leads – perhaps obtained from an agent. For example, these might indicate that a British extremist who travelled to join Daesh in Syria in late 2014, whose full name is not yet known, is trying to make contact with a group of known extremists back in a particular region of the UK. The intelligence might indicate that the group potentially has access to firearms, and may be planning an attack.

5.3. In such cases, the lack of a full identity or any information about specific communications devices means that the security and intelligence agencies cannot use more targeted powers at this stage of the investigation. The analysis of data obtained in bulk is frequently the only means of identifying those involved.

5.4. In pursuing a new lead or in the early stages of an investigation, a common first step for the security and intelligence agencies is to work from a fragment of information to identify individuals of intelligence interest and to establish how they are communicating. Bulk personal datasets and bulk communications data play a very important role in this process. By matching the initial details the security and intelligence agencies have obtained – perhaps part of a name, nationality, and limited information on previous travel – against the passport datasets they hold, the search can be narrowed down to a much smaller list of suspects.

Fig. 5.1 Use of bulk personal datasets to narrow the search


Someone with a particular first name…
…who travelled to a particular country in a certain month…
…and is believed to be in contact with known extremists in a particular postcode.

5.5. In the Syrian example above, the security and intelligence agencies could also use bulk data to begin identifying the UK based individuals, by matching known extremists in the relevant region of the UK against those assessed to have access to firearms.

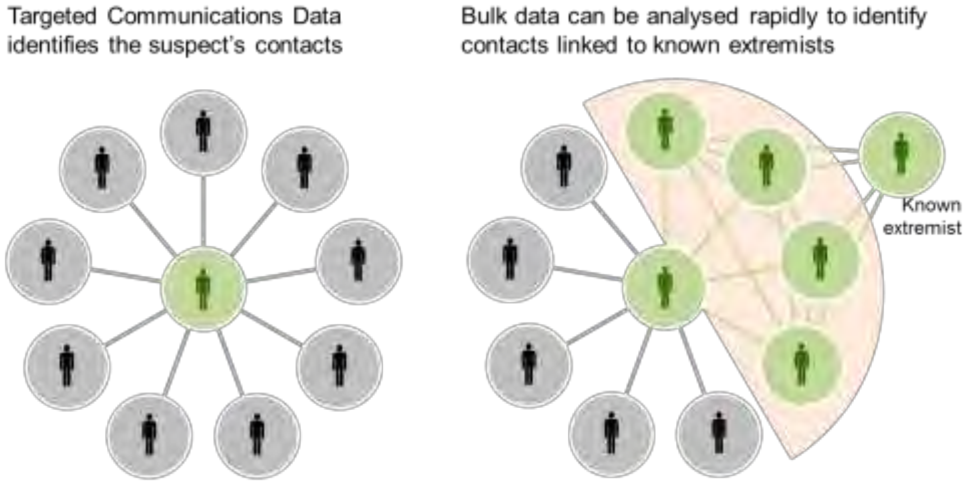
Identifying the wider network

5.6. Often terrorists do not plan attacks by themselves and are part of a larger coordinated group. Once a subject of interest has been identified, analysis of communications data can then be used to identify the people he or she communicates with. By analysing the complex patterns of communications for those numbers, and matching against bulk personal data, the agencies could then identify other UK based members of the cell, for example by searching for links to other known extremists. In contrast, individual requests for communications data to UK communications service providers would provide only a fragmented understanding of whether the subject of interest's associates were of intelligence interest in their own right.

5.7. Using information from communications service providers without the ability to conduct complex analysis of bulk data would also mean that the security and intelligence agencies would need to conduct intrusive analysis against a larger range of individuals in order to assess if they were part of the terrorist network.

5.8. Access to bulk communications data and bulk personal datasets allows the security and intelligence agencies to focus their limited resources on the most serious threats by quickly ruling out other associates and family members from an investigation, and minimising intrusion into the privacy of those who are not of intelligence interest. It can also reduce the risk of an incomplete intelligence picture which makes it difficult to assess the entirety of a threat posed by a known subject – a point made forcefully in the report by the ISC into the murder of Fusilier Lee Rigby in 2013.

Fig. 5.2 Use of bulk communications data to uncover networks


Targeted Communications Data identifies the suspect's contacts
Bulk data can be analysed rapidly to identify contacts linked to known extremists
Known extremist

5.9. This example demonstrates how careful and targeted analysis of bulk data provides an essential way for the security and intelligence agencies to identify links that help prioritise intelligence leads and focus their efforts on individuals or networks that threaten our national security.

Identifying attack planning

5.10. It is not enough to know who is involved in a plot: the security and intelligence agencies also need to know what they are planning in order to disrupt it effectively.

5.11. With the intelligence picture of the network now sufficiently developed, the security and intelligence agencies could seek authorisation to deploy more intrusive techniques, to obtain the content of the group's communications and thus an insight into their attack plans. But without the ability to develop an understanding of the network through the use of bulk data, there would be too many potential subjects of interest, and insufficient intelligence to put forward a case to the Secretary of State for a targeted interception or equipment interference warrant to be considered proportionate.

5.12. However, even when the terrorist network has been identified, in some cases traditional methods for obtaining the content of communications will be ineffective. This means that the security and intelligence agencies may still have only a limited insight into the network's intentions.

5.13. In such cases, bulk communications data analysis could be used to detect an increase in a communications activity that may indicate an attack is being planned. Alternatively, a sudden decrease in activity may indicate that an individual has become more security conscious, as their attack planning has developed. This could trigger further investigation, in which bulk data would play an important role in re-tracing their steps and identifying likely associates.

Identifying threats overseas

5.14. As well as using bulk data to investigate threats in the UK, bulk powers are also used to obtain communications or other data relating to terrorists overseas who are seeking to harm UK citizens. These could be terrorists planning to attack UK nationals overseas, or who are based overseas and intending to conduct an attack in the UK.

5.15. In some cases the UK can work with overseas partners but more often the individuals of intelligence interest are located in failed states, or where the UK has a limited or no physical presence. The use of interception and equipment interference is often the only way to support these investigations.

5.16. It is difficult to acquire, or even identify, the online activities of foreign subjects of interest through targeted interception of their communications. This is due to the fragmentary nature of modern communications routes (as explained in Chapter 3) Instead the security and intelligence agencies need to intercept communications in bulk with a view to obtaining as many fragments of the subject of interest's communications as possible. Bulk interception powers are primarily used for this purpose.

5.17. The security and intelligence agencies can also conduct more complex searches to identify previously unknown subjects of interest outside of the UK. Such searches typically contain multiple elements and only those results matching all elements will then be available for examination. This method minimises the potential for 'false positives'. The security and intelligence agencies will only examine communications where it is necessary and proportionate to do so; this allows analysts to determine which individuals need to be investigated further.

5.18. For example, the security and intelligence agencies might analyse data to identify communications in a conflict zone in order to identify unusual behaviour and potential threats to UK interests in the region. It would be impossible to undertake this activity without intercepting communications in bulk: there will frequently be no other way to identify threats in these places - where the security and intelligence agencies cannot obtain targeted communications or deploy other capabilities such as surveillance or the use of agents.

5.19. Increasingly, because of the growing prevalence of sophisticated encryption, bulk interception provides valuable information but cannot on its own provide access to the communications of terrorists and organised criminal groups. This means that equipment interference powers are important in obtaining such communications. Bulk equipment interference can play an important role in identifying a target's phone or computer from amongst hundreds of possible devices in a particular area from which a terrorist group is plotting, enabling targeted operations to gain access to their communications.

Targeted and bulk: complementary powers

5.20. Bulk data is vital in helping to inform decisions on how best to prioritise and direct finite resources against the most serious threats, where it matters most – often in complex and fast-moving investigations where the difference between a terrorist attack succeeding or being disrupted can be days or even hours.

5.21. The ability to progress investigations quickly and securely through carefully directed, and properly authorised, analysis of bulk data gives the security and intelligence agencies a vital advantage in tackling serious threats.

5.22. The security and intelligence agencies could not achieve the same results in protecting the UK without the use of bulk capabilities:

- in many cases they would not be able to identify threats in the first place: they would be unable to follow up important fragments of intelligence and they would not be able to direct their targeted powers (and finite resources) to the most serious threats;

- in other cases they would not be able to conduct the sophisticated analysis necessary to investigate serious and fast-moving national security threats - using targeted powers alone could not replicate this effect, or deliver at the same pace;

- in the case of bulk interception, without having acquired the data in the first place, it simply would not be available when the security and intelligence agencies need it to investigate and respond to a serious threat.

5.23. In the context of the current threat and communications environment, it is rarely a question of choosing between targeted or bulk powers: the security and intelligence agencies need to use both targeted and bulk capabilities in combination to be able to identify, investigate and disrupt threats to national security.

5.24. Further examples of the use of each of the bulk powers in the Investigatory Powers Bill can be found in Chapters 7 to 10.

6. The Investigatory Powers Bill

6.1. The Investigatory Powers Bill updates the legislation that allows the security and intelligence agencies to use bulk powers to counter threats to the UK. In doing this the Bill will clarify the law, unifying the powers in a single piece of legislation, and strengthen the safeguards which govern the security and intelligence agencies' collection and use of data.

The key provisions in the Bill

6.2. The Bill covers powers to intercept communications, conduct equipment interference, use and retain bulk personal datasets and obtain communications data in bulk. All of these bulk powers are already available to the security and intelligence agencies under existing legislation:

- The Investigatory Powers Bill provides a clear statutory framework for all of the bulk powers available to the security and intelligence agencies and introduces robust, consistent safeguards across all of those powers.

- Only the security and intelligence agencies will be able to apply for any kind of bulk warrant. All bulk interception, communications data and equipment interference warrants must be necessary in the interests of national security.

- The Secretary of State cannot issue a bulk warrant without the prior approval of a Judicial Commissioner.

- The Bill provides that bulk interception and bulk equipment interference warrants may only be issued where the main purpose of the activity is to acquire intelligence relating to individuals outside the UK.

- Additional safeguards will apply in respect of content acquired under bulk interception and bulk equipment interference warrants relating to persons in the UK. If an analyst wishes to examine this data, he or she will need to seek a targeted examination warrant from the Secretary of State and a Judicial Commissioner. This provides exactly the same authorisation as a targeted interception or targeted equipment interference warrant.

- Access to any data obtained under a bulk warrant must be necessary for one or more specific Operational Purposes, as set out on the warrant approved by the Secretary of State and a Judicial Commissioner (see 6.10).

- The draft Bill builds on recommendations made by David Anderson QC and the RUSI panel by allowing the Secretary of State to issue a bulk interception warrant authorising the obtaining of secondary data only. This is data, which can be acquired through interception that does not reveal the meaning of the communication. This provides a less intrusive means of meeting the security and intelligence agencies' information requirements in certain cases when the content of communications is not always required – for example, for certain types of cyber defence work.

Safeguards: The 'double-lock'

6.3. The Investigatory Powers Bill will overhaul the way bulk powers are authorised. In future, warrants for bulk powers will need to be authorised by a Secretary of State and approved by a Judicial Commissioner.

6.4. The Investigatory Powers Commissioner (IPC), supported by Judicial Commissioners, who will hold, or have held, high judicial office, will conduct inspections and investigations to ensure the powers are used appropriately and in full accordance with the law. The IPC will be responsible for ensuring that the detailed safeguards set out in the Bill, as well as Codes of Practice, are adhered to stringently.

6.5. The Commissioner will have the resources, powers and technical expertise available to effectively, and visibly, hold the security and intelligence agencies to account including the ability to initiate their own independent investigations.

Safeguards: How bulk data is controlled

6.6. The Bill will clarify the law underpinning these powers and will make them subject to robust, consistent safeguards. Robust safeguards govern access to any data obtained in bulk in order to protect privacy. Any access to data must be necessary and proportionate.

6.7. It is inevitable that much of the data acquired using any of the bulk capabilities will not be of intelligence interest, because it is impossible to determine at the time of acquisition whether a particular piece of information will have intelligence value. The security and intelligence agencies will always focus and filter their collection as much as possible, on the basis of the most up-to-date assessment of the threats facing the UK. Data is held only as long as is necessary and proportionate.

6.8. The current infrastructure of the internet aggregates huge volumes of traffic from many diverse sources into fibre-optic cables. The volume of communications traffic changes over time, and can do so from minute to minute. This means that in some cases, where the security and intelligence agencies are trying to obtain data relating to communications between individuals in an overseas location of significant intelligence concern, they will also unintentionally, and unavoidably, end up acquiring data from other parts of the world, and potentially data relating to the communications of people in the UK. The Bill provides additional protections for the content of communications relating to people in the UK acquired under bulk interception and bulk equipment interference powers. These are equivalent safeguards that apply to targeted powers.

6.9. The Bill will also require systems to be in place that prevent intelligence analysts from trawling through the data, or accessing every piece of data acquired. The security and intelligence agencies take extremely seriously their responsibility to protect the privacy of individuals whose data has been collected. Bulk data is held securely, and can only be accessed in specific ways by highly trained and security-cleared staff, through controlled queries which pull out only the relevant data. Every query must be necessary and proportionate to meet the intelligence requirement the analyst is working on. Judicial Commissioners and their inspectors can audit these searches to prevent misuse. Arbitrary intrusion would be unlawful.

Operational Purposes – what are they and how will they work?

6.10. All of the provisions for bulk powers in the Bill make clear that examination of any data acquired may only take place for one or more of the Operational Purposes that are specified on the warrant, which must be authorised by the Secretary of State and approved by the Judicial Commissioner.

6.11. Operational Purposes must relate to one or more of the statutory purposes also specified on the warrant (in the interests of national security; for the prevention of or detection of serious crime; and the economic wellbeing of the UK so far as it is also in the interests of national security). Within the ambit of the statutory purposes, Operational Purposes will provide a more detailed description of the purposes for which the data might be examined.

6.12. Since it is likely that data obtained under a bulk warrant might be relevant for many Operational Purposes, any individual bulk warrant may include multiple Operational Purposes. For example, bulk interception and bulk personal data warrants will often specify a range of the security and intelligence agencies' Operational Purposes so that the data can be used across multiple areas of work. The Intelligence and Security Committee of Parliament and the Investigatory Powers Commissioner will have sight of all Operational Purposes.

The full range of Operational Purposes will be highly classified by its nature, as they will contain granular detail. However, they will cover the core functions of each of the agencies' roles, for example:

- Counter Terrorism
- Counter Proliferation
- Countering Hostile Actors
- Safeguarding Prosperity
- Tackling Serious Crime

6.13. Examples of possible Operational Purposes might include:

- **Counter Terrorism**: To detect and disrupt direct threats to the UK and allied interests overseas from Daesh and its affiliates.

- **Counter Terrorism:** To detect and disrupt threats to UK and allied interests overseas from groups with a focus on North and West Africa.

- **Cyber Defence Operations:** To understand the scale and nature of the cyber threat to the UK and allied interests.

- **Serious Crime:** To detect and disrupt child sexual exploitation and abuse.

- **Security of agencies' and allies' operational capability:** To maintain and protect the security and intelligence agencies' and allies' covert capability and infrastructure. To investigate possible threats against such capability and/or infrastructure.

- **Security Assurance:** To provide security awareness to the Government, members of the armed forces, government departments, government agencies, and key government partners, to enable the maintenance and development of protective security practices.

Examination warrants

6.14. Bulk interception and bulk equipment interference are foreign-focused powers. Warrants for these powers must target overseas-related communications and must not be sought in order to obtain the communications or data of people in the UK. Due to the nature of modern communications, it is impossible to ensure that bulk interception and bulk equipment interference do not incidentally acquire some communications between, or private information of, individuals in the UK. If such data has been acquired, the Investigatory Powers Bill requires that the content of the communications or private information can only be selected for examination once the analyst has obtained a targeted examination warrant.

6.15. A targeted examination warrant will be subject to the same 'double-lock' authorisation process as a targeted interception or targeted equipment interference warrant. This requires the warrant to be authorised by a Secretary of State and approved by a Judicial Commissioner before it issues.

6.16. Strict safeguards govern any examination of secondary data: any examination must be necessary and proportionate for a specific Operational Purpose authorised under the warrant. Compliance is subject to retrospective audit by both agency staff and the Judicial Commissioners. Misuse of these powers can result in criminal prosecution.

THE POWERS IN DETAIL

7. Bulk interception

7.1. Bulk interception is a capability designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK. It allows the security and intelligence agencies to intercept the communications of individuals outside the UK and then filter and analyse that material in order to identify communications of intelligence value.

7.2. Bulk interception is essential because the security and intelligence agencies frequently have only small fragments of intelligence or early, unformed, leads about people overseas who pose a threat to the UK. Equally, terrorists, criminals and hostile foreign intelligence services are increasingly sophisticated at evading detection by traditional means. Just as importantly, due to the nature of the global internet, the route a particular communication will travel is hugely unpredictable. Combined, this means that sometimes the data acquired via bulk interception is the only way the security and intelligence agencies can gain insight into particular areas and threats. Access to large volumes of data is therefore essential to enable communications relating to subjects of interest to be identified and subsequently pieced together in the course of an investigation.

7.3. Bulk interception is not, however, about trying to acquire all of the traffic on the internet: it would not be proportionate, nor would it be an effective way to meet the UK's intelligence requirements. GCHQ's bulk interception systems operate on a very small percentage of the infrastructure that makes up the global internet. They filter this traffic still further using a range of criteria to focus on that most likely to meet their approved Operational Purposes. Robust access controls then mean that communications are only examined by an analyst when it is necessary and proportionate.

Current Position

7.4. Bulk interception is provided for under section 8(4) of the Regulation of Investigatory Powers Act 2000 (RIPA). Under the current regime, a warrant issued by the Secretary of State must consider the necessity and proportionality of the proposed interception and whether the information collected through interception could reasonably be obtained by other means. An interception warrant issued under section 8(4) of RIPA must be accompanied at the time of its issue by a certificate, also issued by the Secretary of State, certifying a description of intercepted material the examination of which is considered necessary. The conduct authorised by an interception warrant issued under 8(4) must be confined to the interception of "external communications", defined as those which are sent or received outside the British Islands.

7.5. Conduct authorised under a section 8(4) warrant may sometimes result in the incidental interception of communications that were both sent and received in the British Islands; RIPA permits this only if it is necessary to intercept the external communications that are the target of the warrant. Before material intercepted under a section 8(4) warrant may be selected for examination, it is subject to a further consideration of necessity and proportionality. If an analyst wishes to select for examination the content of the communications of an individual known to be located in the British Islands, he or she must apply to the Secretary of State for an authorisation under section 16(3) of RIPA. This process is similar to the application for a warrant under section 8(1).

Safeguards in the Bill

7.6. The Investigatory Powers Bill will maintain the security and intelligence agencies' capabilities to undertake bulk interception without introducing any new powers. Bulk interception warrants will continue to be limited to the security and intelligence agencies, and there will continue to be strict safeguards governing its use, which ensure the security and intelligence agencies comply fully with their human rights obligations.

7.7. Bulk interception warrants must be foreign-focused and their main purpose must be limited to the interception of overseas-related communications or secondary data.

7.8. The Bill will introduce new safeguards in relation to bulk interception warrants. Bulk interception warrants will continue to be issued by the Secretary of State but will now also need to be approved by a Judicial Commissioner. This will provide the new 'double-lock' authorisation procedure. Warrants for bulk interception will last up to six months. The Secretary of State can renew a warrant if it continues to be necessary and proportionate and the Judicial Commissioner approves it.

7.9. Bulk interception warrants can only be issued in relation to three statutory purposes: in the interests of national security, for the prevention or detection of serious crime and in the interests of the economic well-being of the UK, where there is also a direct link to national security. National security must always be one of the statutory purposes for which a bulk interception warrant is authorised. This ensures that bulk interception is only used when it is required in the interests of national security.

7.10. Any application for a bulk interception warrant must contain a consideration of necessity and proportionality, and will need to set out specified Operational Purposes which govern the way in which intercepted material can be examined. No intercepted data may be selected for examination unless it is proportionate and doing so is necessary for one or more of the Operational Purposes. Those specific purposes must be approved by a Secretary of State and a Judicial Commissioner. More detail on Operational Purposes can be found in Chapter 6.

7.11. Bulk interception should not be undertaken if the information could be obtained by another less intrusive method. Therefore, bulk interception warrants will only be sought and granted where information cannot reasonably be acquired via other means.

7.12. The draft Bill builds on recommendations made by David Anderson QC and the RUSI panel by allowing the Secretary of State to issue a bulk interception warrant authorising the obtaining of secondary data only. This is data that can be acquired through interception but does not include the meaning of the communication. This will provide a less intrusive means of meeting the security and intelligence agencies' information requirements for certain activities where the content is not always required – for example, to investigate particular types of activity on a network and identify malicious activity for the purposes of cyber defence.

7.13. As currently, the global nature of modern online communications means that activity authorised under a bulk interception warrant may incidentally intercept the communications between individuals in the UK. However, the content of communications of any person known to be in the UK may only be selected for examination under the Bill when a targeted examination warrant under Part 2 of the Bill has been obtained. The process for the authorisation of a targeted examination warrant will be the same as that for a targeted interception warrant: it will need to be issued by the Secretary of State having been first approved by a Judicial Commissioner.

7.14. A statutory Code of Practice will set out the handling, retention, destruction and audit arrangements for the data obtained by bulk interception.

7.15. Bulk interception powers will be overseen by the Investigatory Powers Commissioner. The Commissioner will audit the intercepting agencies in order to monitor compliance with the legislation and publish his or her findings in an annual report. Anyone who believes that they may have been subject to unlawful interception can complain to the Investigatory Powers Tribunal to review their case.

Case Studies and Examples

Case Study: Counter-Terrorism

The security and intelligence agencies' analysis of bulk data uncovered a previously unknown individual in 2014, in contact with a Daesh-affiliated extremist in Syria, who was suspected of involvement in attack planning against the West. As this individual was based overseas, it is very unlikely that any other intelligence capabilities would have discovered him. Despite his attempts to conceal his activities, the agencies were able to use bulk data to identify that he had recently travelled to a European country. Meanwhile, separate intelligence suggested he was progressing with attack planning. The information was then passed by the agencies to the relevant national authorities. They disrupted the terrorists' plans and several improvised-explosive devices were seized.

Case Study: Disrupting Child Sexual Exploitation

In 2013, the agencies carried out analysis of bulk data to identify patterns of behaviour used by paedophiles on-line. They identified a UK national visiting a website that sold images of child sexual exploitation. The website was hosted in a country that rarely cooperated with UK law enforcement and without the analysis of bulk data the indivudal's use of the website would have escaped detection. The individual had previously held a position that provided him with access to children, and he was already on the UK Violent and Sexual Offenders register. Due to the security and intelligence agencies' work he was prosecuted for his actions, sentenced to three years' imprisonment and made subject to a Sexual Offenders Harm Order for life.

Case Study: Protecting the UK from cyber attack

The security and intelligence agencies routinely use bulk interception to detect cyber-attacks against the UK, including large scale thefts of data and serious fraud by cyber criminals, and operations by hostile intelligence services and potential terrorists. Using electronic 'signatures', which operate in a similar way to electronic fingerprints, the agencies scan the technical detail of internet communications for evidence of incoming attacks to the UK. This approach can both identify known forms of computer malware and discover new forms of cyber-attack that the agencies have not previously encountered. Cyberspace is so large, and technical change so rapid, that bulk interception is the only way for the agencies to monitor for such attacks as they occur: targeted approaches would be highly likely to miss an attack. The resulting intelligence is typically shared with industry partners, who in turn use it to protect UK citizens and businesses.

8. Bulk Equipment Interference (EI)

8.1. Wherever possible, the security and intelligence agencies have used targeted capabilities to respond to threats to national security. These capabilities have been, and will continue to be, crucial as a means of understanding more about a known subject of interest's intentions. However, they have limitations. The security and intelligence agencies can no longer assume that a terrorist or criminal will use a specific phone or application; or that the data collected from targeted capabilities will reveal the full extent of a plot. Terrorists, serious criminals and hostile states have embraced technological advancements, including the widespread use of encryption, and the growth of the internet to hide from sight and to plan their attacks. As a result of this, the security and intelligence agencies can no longer rely solely on interception and are faced with an increasingly partial and fragmented intelligence picture, even when investigating known threats. If the security and intelligence agencies are to be able to maintain the same understanding of threats and be able to disrupt them, they need to use other, and complementary, techniques which will provide comparable pieces of the intelligence jigsaw.

8.2. Bulk EI describes a set of techniques to obtain information from devices that is necessary for the identification of subjects of interest who pose a threat to the UK's national security, in circumstances where the information is not available through the use of other methods. Bulk EI enables the security and intelligence agencies to overcome techniques used by subjects of interest to hide their identities or their communications. A bulk EI warrant must be foreign-focused and its main purpose must be to obtain data relating to overseas-related communications, equipment data or other information.

Current position

8.3. The security and intelligence agencies have the power to undertake EI operations through the Intelligence Services Act 1994 (ISA), and, in February 2015, the Government published a draft Code of Practice setting out the strong safeguards that the security and intelligence agencies must apply to EI activities. GCHQ's use of computer network exploitation, which is subject to this Code, was upheld as lawful by the Investigatory Powers Tribunal in February 2016.

8.4. ISA authorisations may be for any of the security and intelligence agencies' statutory purposes and are issued by the Secretary of State. Section 7 of ISA permits the issuing of class authorisations which do not require the authorisation to name or describe a particular piece of equipment, or an individual user of the equipment. They are overseen by the Intelligence Services Commissioner.

Bulk EI or Thematic EI

8.5. There are clear and important distinctions between bulk EI and targeted 'thematic' EI operations. These are outlined in the draft EI Code of Practice. Bulk EI includes the additional safeguards of the bulk regime and is an important capability in its own right. Both bulk EI and targeted 'thematic' EI operations can take place at scale, if the relevant criteria are met. It is entirely possible for a targeted 'thematic' EI warrant to cover a large geographic area or involve the collection of a large volume of data. A bulk EI warrant is likely to be required in circumstances where the Secretary of State or Judicial Commissioner is not be able to assess the necessity and proportionality to a sufficient degree at the time of issuing the warrant. The additional access controls at the examination stage are required to ensure the necessity and proportionality of any interference that cannot be assessed fully at the outset. This might be for example where the purpose of the operation is target discovery and the security and intelligence agencies do not know in advance the identity of the new subjects of interest who threaten the security of the UK and its citizens.

8.6. Conversely, a targeted 'thematic' warrant would be appropriate where a greater degree of targeting or filtering can limit interference. In such cases the Secretary of State and the Judicial Commissioner are likely to be able to adequately foresee the proposed interferences with privacy in relation to the data to be examined to a sufficient degree, such that the additional access controls under the bulk EI warrantry regime are not required.

8.7. For bulk EI warrants, further safeguards will be applied to the examination of communications and information of individuals within the British Islands – a separate targeted examination warrant, subject to the full 'double-lock' authorisation is required. As with bulk interception, only a very small portion of the data gathered through bulk EI will ever be selected for examination via robust access controls. To carry out unduly intrusive, reckless, or irresponsible operations would be unlawful. It is essential that these operations do not expose the target device to potential exploitation by third parties, both to protect the privacy of the owner of a device, and to protect the sensitive capabilities used by the security and intelligence agencies.

8.8. The hypothetical scenario below illustrates the difference between targeted 'thematic' EI warrants and bulk EI warrants.

> **<u>Scenario</u>: Intelligence suggests that a Daesh inspired cell in a particular location in the Middle East is plotting an imminent bomb attack against UK interests in the region. The intelligence requirement is for the security and intelligence agencies to find and identify all the individuals in the cell as fast as possible and uncover their plans. To do this, the communications of the individuals in the cell need to be acquired.**

Example 1

Interception reveals that the cell are all using a unique anonymisation package to hide their online identities.

An EI warrant is used to obtain a high volume of equipment data (not content) from a large number of devices in the specified location in the Middle East. By applying a search term (a ‘selector’), that is unique to the anonymisation package, to the ‘pot’ of data collected only data relating to the cell members is retrieved for examination. From this information, the content from only the cell members’ devices can then be collected and examined.

In this example, a specific identifier (the selector unique to the anonymisation package) which is connected directly to the cell members is known from the outset. Accordingly, despite the precise identities of the individuals being unknown, the Secretary of State:

- knows and can fully assess all of the interferences with privacy that will occur (both in relation to the cell members and innocent individuals whose devices will be affected) from the start to the end of the operation;

- knows what will happen at the beginning of the operation to collect the initial ‘pot’ of data; and

- knows, to a high degree of certainty given the specific identifier that will be applied to that ‘pot’, that the communications to be retrieved from the ‘pot’ and examined will belong to the cell members.

As the cell members can be identified from their association to a specific, known anonymisation package, a targeted ‘thematic’ warrant is suitable.

Example 2

By contrast with Example 1, little is known about the individual members of the terrorist cell. No technical details are known about their communications or the devices they are using. However, it is known that a particular software package is commonly – but not exclusively – used by some terrorist groups.

An EI warrant is used to obtain a large volume of equipment data (not content) from a large number devices in the specified location in the Middle East. Using a specific search term (a ‘selector’) related to the software package, data relating to the users of the software package is retrieved from the ‘pot’ of data collected.

Analysts apply other search terms and analytical techniques to the data to find common factors that indicate a terrorist connection. The results show that some people from the original ‘pot’ (those using the software package associated with terrorists) have also accessed a particular Internet Protocol (IP) address which is known to be linked to an extremist website containing among other things, a bomb-making manual. Using the newly discovered IP address, the original ‘pot’ of data is searched again to find other devices that have also accessed the website. A series of refined searches of this kind will gradually identify devices that belong to the terrorist cell. Their communications (including content) can then be collected and examined.

By contrast with Example 1, no identifiers which relate solely to the targeted individuals are known from the outset. The only identifier known at the outset is the software package used by terrorists but also by some other, innocent, individuals. The IP address linked to the extremist website and the other refining factors were only uncovered during the course of the operation through analysis of the original ‘pot’ of data.

Consequently, the Secretary of State cannot know nor fully assess all of the interferences with privacy that will occur (both in relation to the cell members and innocent individuals whose devices will be affected) from the start to the end of the operation. The Secretary of State knows:

- the objective and the scale of the operation and what will be done in order to collect the initial ‘pot’ of data;

- that the information to be retrieved from the ’pot’ of data will likely include the data of terrorists, that will lead to the cell, but also some data belonging to innocent individuals (given the software package is not exclusively used by terrorists); and

- that further analytic work will be required leading to more refined searches on the initial ‘pot’ in order finally to discover and obtain the communications of the terrorist cell.

But at the point of issuing the warrant, the Secretary of State is not in a position to assess the necessity and proportionality of subsequent searches of the ‘pot’. To ensure that all of those searches are carried out in accordance with privacy considerations, additional examination safeguards need to be in place.

As the cell members can only be identified following considerable target discovery effort, a bulk EI warrant is suitable.

Safeguards in the Bill

8.9. The Investigatory Powers Bill reflects the increasing need to adopt the approach outlined in the examples above and provides a more transparent statutory basis for its use along with clear safeguards.

8.10. The bulk EI provisions in the Investigatory Powers Bill detail when equipment interference may be used and set out enhanced safeguards that apply to the use of that power.

8.11. As is the case with a bulk interception warrant, a bulk EI warrant must be foreign-focused and its main purpose must be limited to obtaining data relating to overseas-related communications, equipment data or other information. These are defined as those communications sent or received by individuals outside the UK, or the information of individuals who are outside the UK. Bulk EI warrants will be limited to the security and intelligence agencies, and there will continue to be strict safeguards governing its use, which ensure the security and intelligence agencies comply fully with their human rights and data protection obligations.

8.12. The Bill will also introduce new safeguards in relation to the authorisation of bulk EI warrants. Bulk EI warrants will have to be issued by the Secretary of State and that decision must also be approved by a Judicial Commissioner beforehand. This will provide a new ‘double-lock’ authorisation safeguard. Warrants for bulk EI will last up to six months. The Secretary of State can renew a warrant if it continues to be necessary and proportionate and the Judicial Commissioner approves that decision.

8.13. As is the case for bulk interception, bulk EI warrants can only be issued in relation to three statutory purposes: in the interests of national security, for the prevention or detection of serious crime and in the interests of the economic well-being of the UK, where there is also a direct link to national security. National security must always be one of the statutory purposes for which a bulk EI warrant is authorised, this ensures that bulk EI is only used when it is required in the interests of national security.

8.14. Any application for a bulk EI warrant must contain a consideration of necessity and proportionality, and will need to set out the specified Operational Purposes that the data obtained under the warrant can be examined for. Those specific purposes must be approved as being necessary by a Secretary of State and a Judicial Commissioner. More detail on Operational Purposes can be found in Chapter 6.

8.15. The Bill requires that bulk EI must not be undertaken if the information could be obtained by another less intrusive method.

8.16. The global nature of modern online communications and devices means that activity authorised under a bulk EI warrant may incidentally obtain the information of individuals in the UK. The Bill will provide for additional safeguards to cover this possibility. The content of an individual known to be in the UK may only be selected for examination when a targeted examination warrant has been obtained. The process for the authorisation of a targeted examination warrant will be the same as that for a targeted EI warrant: it will need to be issued by the Secretary of State and approved by a Judicial Commissioner.

8.17. A statutory Code of Practice will set out the handling, retention, destruction and audit arrangements for the data obtained by bulk EI.

8.18. The use of bulk EI powers will be overseen by the Investigatory Powers Commissioner. The Commissioner will audit the security and intelligence agencies in order to monitor compliance with the legislation (including the Code of Practice) and publish the findings in an annual report. Anyone who believes that they may have been subject to unlawful equipment interference can complain to the Investigatory Powers Tribunal to review their case.

Case Studies and Examples

Example: Protecting Against a Terrorist Attack

A group of terrorists are at a training camp in a remote location overseas. The security and intelligence agencies have successfully deployed targeted EI against the devices the group are using and know that they are planning an attack on Western tourists in a major town in the same country, but not when the attack is planned for. One day, all of the existing devices suddenly stop being used. This is probably an indication that the group has acquired new devices and gone to the town to prepare for the attack. It is not known what devices the terrorists are now using. The security and intelligence agencies would use bulk EI techniques to acquire data from devices located in the town in order to try to identify the new devices that are being used by the group. If it is possible to identify those devices quickly enough, it may be possible to disrupt the attack. Without bulk EI powers, it is very unlikely that this would be achievable.

Example: Countering Biological Weapons Proliferation

A hypothetical totalitarian state has an indigenous email system which is mandated for use by the general population, but also by scientists working on the state's biological weapons programme who are involved in the proliferation of weapons technology. This means it is used by many thousands of people within that country. The security and intelligence agencies can only obtain limited data from interception which means it is not possible to identify particular accounts which belong to individuals of intelligence interest working on the biological weapons programme. Bulk EI techniques would be needed to access a limited amount of data relating to a very large number of users of the service – potentially even all its users. This would enable the security and intelligence agencies to filter out those who were not of intelligence interest, and focus on those who were associated with the biological weapons programme in order to use targeted EI techniques against them to support the UK's aim of disrupting their proliferation of biological weapons.

Example: Cyber Defence

A state controlled agent provides the infrastructure to several other state controlled malicious Computer Network Exploitation (CNE) programmes. These programmes are responsible for espionage against the Government and UK industry at massive scale. The security and intelligence agencies' ultimate aim would be to identify that agent and any others supplying infrastructure to the programmes in order to find any of the new computer equipment before it is used.

In order to do this the security and intelligence agencies would need to use bulk EI to survey a location from where they believe the infrastructure is being procured, in order to identify activity characteristic of the procurers. In order to find these individuals, the security and intelligence agencies would need to acquire a large amount of data from which to identify likely candidates, who would then be subject to more targeted intelligence investigation.

9. Bulk acquisition

9.1. Fast, secure access to bulk communications data is essential to the security and intelligence agencies in pursuing their investigations. Bulk communications data has played a part in every major counter terrorism operation over the last decade. It is a crucial investigative tool that the security and intelligence agencies use on a daily basis as they work to identify and disrupt the most serious threats facing the UK.

9.2. The ability to acquire and access this data in bulk, subject to strict safeguards and oversight, is vital to the security and intelligence agencies' effectiveness. It has helped stop terrorist attacks and to save lives.

9.3. Bulk communications data enables the security and intelligence agencies to identify and investigate potential threats in complex and fast-moving investigations. It allows the security and intelligence agencies to conduct more sophisticated analysis, by 'joining the dots' between individuals involved in planning attacks, often working from fragments of intelligence obtained about potential attacks:

- Carefully directed searches of bulk communications data in complex investigations and operations can identify frequent contact between subjects of interest and their associates, including potential attack planning activity.

- Identifying those links between individuals or groups can help to direct where a warrant for more intrusive acquisition of data, such as interception, is needed.

- Bulk communications data allows searches to be conducted for traces of activity by previously unknown suspects who surface in the course of an investigation, helping to identify further potential threats that require investigation.

9.4. In some cases bulk communications data may be the only investigative lead that the security and intelligence agencies have to work with. While the security and intelligence agencies can also make individual communications data requests to communication service providers, the ability to access data in bulk is critical, because it enables the security and intelligence agencies to conduct searches, where necessary and proportionate, across all the relevant data, in a secure way.

9.5. This enables more complex analysis to be undertaken, particularly when the results are matched against other data holdings – for example, that held in bulk personal datasets. By using bulk communications data, links can be established that would be impossible or significantly slower (potentially taking many days) to discover through a series of individual requests to communication service providers. This can sometimes be the difference between identifying and disrupting a plot, and an attack taking place.

9.6. It also enables the security and intelligence agencies to narrow down likely targets much more quickly, so that they can focus limited investigative resource where it is really needed. Without access to bulk communications data, the security and intelligence agencies would be much less able to concentrate their efforts on those who pose the greatest threat, and without the benefit of this insight there would be a significantly greater risk of intruding into the lives of innocent individuals during the course of investigations as the security and intelligence agencies work to narrow down possible suspects.

Current Position

9.7. There is an existing power for the Secretary of State to issue directions to communications service providers under section 94 of the Telecommunications Act 1984 which has enabled the security and intelligence agencies to obtain communications data in bulk. This has been approved by successive governments. The capability was first used at scale in the UK in 2001 after the 9/11 attacks in New York, and later extended following the attacks on the London transport system on 7 July 2005 to respond to the domestic terrorist threat. Directions issued under this power are reviewed every six months and, as the Prime Minister stated in March 2015, the Interception of Communications Commissioner provides oversight of the use of section 94.

Safeguards in the Bill

9.8. Bulk acquisition warrants, used to acquire bulk communications data, will be subject to the new ‘double-lock’ authorisation process, so both a Secretary of State and a Judicial Commissioner will review the application.

9.9. Only the security and intelligence agencies will be able to apply for a bulk acquisition warrant.

9.10. The security and intelligence agencies may only apply for a bulk acquisition warrant in relation to three statutory purposes: in the interest of national security, for the prevention and detection of serious crime and in the interest of the economic well-being of the UK where there is also a direct link to national security.

9.11. National security must always be one of the statutory purposes for which a bulk acquisition warrant is authorised.

9.12. The warrant will also need to set out the specified Operational Purposes for which the data collected can be selected for examination. Those specific purposes will also be approved by both Secretary of State and a Judicial Commissioner and might include, for example, “attack planning by Daesh in Syria against the UK”. No data may be selected for examination except for those purposes.

9.13. Bulk acquisition warrants must be served on a communications service provider. The power cannot be used by an intelligence agency to acquire communications data from a telecommunication system themselves.

9.14. Bulk acquisition powers will be overseen by the Investigatory Powers Commissioner. The Commissioner will audit the security and intelligence agencies in order to monitor compliance with the legislation and publish his or her findings in an annual report. Anyone who believes that there may have been unlawful acquisition or use of bulk communications data by the security and intelligence agencies can complain to the Investigatory Powers Tribunal to review their case.

Case Studies and Examples

Case Study: Protecting Northern Ireland

Within the last three years, a group of terrorists were planning an attack in Northern Ireland. It was suspected that they had already obtained explosives for the attack and were escalating their activity. Increased activity often indicates that an attack is close, but in this case the exact date was not known and the group's attention to security made it extremely difficult to discover more.

Bulk communications data provided the breakthrough. Through interrogation of the data, the security and intelligence agencies found previously unknown members of the network and were able to increase their coverage of this expanded group. As a result they became aware of a sudden further increase in activity from analysis of the group's communications activity. This led to police action and the recovery of an improvised explosive device.

It was clear that the device was ready for use and the increased activity was most likely late-stage preparation for the attack. The security and intelligence agencies' work, built upon analysis of bulk communications data, provided sufficient grounds for the police to arrest a key figure in the plot, who was subsequently charged and convicted with terrorism offences.

Case Study: Preventing bombings in the UK

In 2010, a group of terrorists were plotting bombings at several symbolic locations in the UK, including the London Stock Exchange. Following an intensive investigation, in which analysis of bulk communications data played a key role, not least as the network was spread across multiple locations, the group were all identified and their plot uncovered. The investigation required the complex analysis of large volumes of data in order to identify the attackers and to understand the links between them; it would not have been possible to do this at speed by relying on requests for targeted communications data.

The security and intelligence agencies were then able to work with police to disrupt them in time and the group were charged with terrorism offences, including conspiracy to cause an explosion. All entered a guilty plea and were sentenced to prison terms of up to 18 years.

Case Study: Preventing a kidnap

The security and intelligence agencies uncovered a plot by known terrorists to stage a kidnap. This plan was still in the early stages, which meant that immediate efforts to arrest the plotters risked not having sufficient evidence to convict them successfully. On the other hand, if the police and intelligence agencies had acted too late, the group might have been able to carry out their plan. A solution was therefore required which balanced these two risks.

The security and intelligence agencies were able to use communications data to analyse patterns of communications between members of the group. This enabled them to assess the risks, so that appropriate action could be taken to ensure the safety of the potential victim and their family, who were relocated while the investigation continued. The group were prevented from carrying out their plan and those who had been targeted were able to return home.

Catching and prosecuting attackers

Example 1: Following a failed terrorist attack in London in 2007, the security and intelligence agencies were able to confirm that the perpetrators were the same as a group who had carried out another attack shortly afterwards. This was achieved in a matter of hours through the analysis of bulk communications data, and was vital in understanding the scale of the threat posed in a fast-moving post-incident investigation, because of the ability to identify connections at speed; it would not have been possible to do this at speed by relying on requests for targeted communications data.

Through further analysis of communications data, the investigation went on to identify people who had had extensive contact with telephones used in the London attack. This enabled the security and intelligence agencies and police to establish at speed, that no further attacks were planned. The operation led to a successful prosecution.

Example 2: A group of terrorists were planning to kidnap and murder a British Muslim solider in the UK in 2007. They intended to video the soldier's death and send the film to their terrorist contacts abroad for public release. Bulk communications data allowed the security and intelligence agencies to identify the group from patterns of communication activity. This paved the way to the police searching their properties, where a number of items were recovered which confirmed they had indeed been planning a kidnap and murder. This resulted in successful convictions. Bulk communication data was critical to this outcome.

As the group was unknown at the outset of the investigation, relying on targeted data would have required the security and intelligence agencies to proceed much more slowly in order to identify potential members of the group and to discount others from their investigations. The ability to analyse bulk data meant that this process was faster and more effective.

Case Study: Thwarting mass casualty attacks against aviation

In 2006 a group of terrorists based in more than one part of the UK plotted to bring down multiple aircraft using homemade bombs (improvised explosive devices). If successful, their plan would have been the largest terrorist attack ever to take place in the UK, with a death toll similar to the 9/11 attacks in the United States. The security and intelligence agencies used bulk communications data to find these terrorists and disrupt their plan. This required the complex analysis of large volumes of data in order to identify the attackers and to understand the links between them; it would not have been possible to do this at speed by relying on requests for targeted communications data.

Those planning the attack were arrested, tried and sentenced to life imprisonment.

10. Bulk Personal Datasets (BPD)

10.1. Bulk personal datasets comprise personal data relating to a number of individuals, the majority of whom are unlikely to be of intelligence interest. The security and intelligence agencies hold the data electronically and analysts will only look at the data relating to the minority who are of intelligence interest. The security and intelligence agencies do this by asking specific questions of the data to retrieve information of intelligence value.

10.2. The analysis of BPD by the security and intelligence agencies is a critical part of their response to the increasingly complicated and challenging task of defending the UK's interests and protecting its citizens in a digital age.

10.3. It is an essential tool that is used on a daily basis, in combination with other capabilities, right across the security and intelligence agencies' operations. It plays an integral role in enabling the security and intelligence agencies to exercise their statutory functions. Without it, the security and intelligence agencies would be significantly less effective in protecting the UK against threats such as terrorism, cyber threats or espionage.

10.4. BPD enables the security and intelligence agencies to focus their efforts on individuals who threaten our national security or may be of other intelligence interest, by helping to identify such individuals without using more intrusive investigative techniques. It helps to establish links between subjects of interest or better understand a subject of interest's behaviour. BPD also assists with the verification of information obtained through other sources (for example agents) during the course of an investigation or intelligence operation.

10.5. Travel data, for example, helps the security and intelligence agencies to establish an understanding of the travel history of a subject of interest which, in turn, enables them to disrupt the activities of those who mean us harm.

10.6. Using BPD also enables the security and intelligence agencies to use their resources more proportionately because it helps them exclude potential suspects from more intrusive investigations.

10.7. A list of people who have a passport is a good example of a BPD that the security and intelligence agencies might hold - it includes personal information about a large number of individuals, the majority of which will relate to people who are not of interest to the security and intelligence agencies. Other examples of BPD might include population data (such as the electoral register), commercial data, data relating to communications (such as the telephone directory), financial data (such as data relating to suspicious financial activity), and data acquired from other intelligence or law enforcement agencies (such as data about individuals with access to firearms).

Current position

10.8. The use of BPD is not new, and the Bill does not provide new powers for acquiring bulk personal datasets. The power to acquire BPD comes from section 2(2)(a) of the Security Service Act 1989 (SSA) and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 (ISA) – sometimes referred to as the 'information gateway provisions'. These provisions allow the security and intelligence agencies to acquire information only where it is necessary and proportionate for the proper discharge of their statutory functions, and are the primary statutory route by which they obtain bulk personal datasets.

10.9. BPDs may also be acquired using statutory investigatory powers (e.g. interception and equipment interference), from other public sector bodies or commercially from the private sector.

10.10. The use of BPD is subject to stringent internal handling arrangements and is overseen by the Intelligence Services Commissioner, who confirmed in his 2014 report that *"the case for holding BPD has been established in each service"* and *"agencies all have strict procedures in place in relation to handling, retention and deletion. Misuse of data is fortunately rare. My experience is that officers work with a high degree of integrity and an awareness that the systems they have access to contain highly sensitive information which must be protected."*

Safeguards in the Bill

10.11. The Bill will provide a robust and transparent regime for retaining and using BPD.

10.12. The Bill provides for significant new safeguards. The most significant is the requirement to obtain warrants to retain and use BPDs. As is standard for warrants in the Bill, they will last six months and they will be subject to the 'double-lock' safeguards such that a Secretary of State must be satisfied that the warrant is necessary and proportionate and the Judicial Commissioner must approve its issuance. The Secretary of State must also be assured that there are satisfactory arrangements in place to store the data securely. There will be two types of warrant in the Bill – class BPD warrants and specific BPD warrants.

10.13. Class BPD warrants will authorise the retention and use of a particular class of BPD. Class BPD warrants are for those datasets which are similar in their content and proposed use and raise similar considerations as to, for instance, the degree of intrusion and sensitivity, and the proportionality of using the data. This allows the Secretary of State to consider the necessity and proportionality of acquiring all data within the relevant class: a class warrant might, for example, authorise an agency to acquire travel datasets that relate to similar routes and which contain information of a consistent type and level of intrusiveness.

10.14. Specific BPD warrants will authorise the retention and use of a specific dataset. Before a decision is made as to the type of warrant that is appropriate, the agency will assess (amongst other things) whether the data is already publicly available and whether it includes sensitive personal data which would be considered more intrusive. The BPD Code of Practice sets out further details of the factors which need to be taken into account. If a dataset is assessed – by reference to these factors – to contain a significant component of intrusive data, it will have to be authorised by a specific BPD warrant.

10.15. Any warrant application for use of a BPD must also set out specified Operational Purposes. No data held within the BPD may be examined unless it has been deemed necessary and proportionate by the Secretary of State and the Judicial Commissioner to do so, for one or more of the Operational Purposes stipulated on the warrant. More detail on Operational Purposes can be found in Chapter 6. It is likely that a security and intelligence agency will, in applying for a class BPD warrant, make the case for many or all of their Operational Purposes to apply. This is because BPDs facilitate 'joining the dots' across investigations and operations: it is not always known in advance which particular BPD will contain the vital missing 'dot' in an investigation.

10.16. A new statutory Code of Practice will set out the handling, retention, destruction and audit arrangements for BPD.

10.17. The Investigatory Powers Commissioner will review the acquisition, retention, use or disclosure of BPD by the security and intelligence agencies. The Commissioner will audit how the security and intelligence agencies use them and will report publicly on the findings annually.

Case Studies and Examples

Case Study: Focusing investigative resources

Intelligence indicated that a partially identified associate of a known subject of interest aspired to travel to Syria for extremist purposes. Using BPD, agency analysts were quickly able to identify the associate, enabling rapid focus of investigative effort on the one individual of concern and discounting hundreds of other potential candidates. Without access to BPD, a resource intensive and more intrusive process would have been needed to identify the individual from the hundreds of potential candidates, incurring collateral intrusion into individuals of no intelligence interest and with significant risk of failing to identify the individual prior to travel.

Case Study: Stopping Al Qaeda (AQ) terrorist plots

Intelligence received by the security and intelligence agencies indicated that a member of AQ was facilitating suicide bombers in the UK. The security and intelligence agencies had a broad description for the AQ member but no name. Potential contact information was received, but didn’t immediately identify the individual. Using BPD analysts were able to identify possible matches and quickly narrow this down to one strong match. At this point the necessity and proportionality case was robust enough to deploy other, more intrusive methods to cross-check the information and positively identify that the match was the suspected AQ member.

Case Study: Identifying foreign fighters

Timely access to travel data has provided advance notice of the unexpected return to the UK of people judged to pose a potential threat to UK security. This helps the security and intelligence agencies to prepare a tailored response prior to their arrival to better mitigate the threat they pose to national security. Information derived from travel data has also been critical to the ability of the security and intelligence agencies and their international partners to identify individuals travelling to join Daesh in Syria and Iraq and then disrupt their activities, including when they return to the UK radicalised.

Case Study: Identifying subjects of interest

The name of an individual reported to be storing a weapon used in a terrorist attack was identified by the security and intelligence agencies. A combination of BPD were used to fully identify this person from hundreds of possible candidates. This resulted in the recovery of the weapon, and aided in the subsequent conviction of the individuals involved in the terrorist attack, who are now serving lengthy prison sentences.

Case Study: Preventing terrorist access to firearms

The risks of terrorist access to firearms have been highlighted by tragic events in Mumbai, Copenhagen and more recently Paris. To help manage the risk of UK based subjects of interest accessing firearms, the security and intelligence agencies match data about individuals assessed to have access to firearms with records of known terrorists. To achieve this, the security and intelligence agencies acquired multiple datasets that contained the details of individuals who may have access to firearms, even though the majority will not be involved in terrorism and therefore will not be of security concern. This allows the matching to be undertaken at scale and pace, and more comprehensively than individual requests could ever achieve. This in turn has enables the security and intelligence agencies to manage the associated risks to the public.

Case Study: Identifying human intelligence agents

The security and intelligence agencies were tasked by the UK's Joint Intelligence Committee to produce intelligence on a specific country threatening the UK's national security. They identified an individual with access to the required intelligence, but were unable to approach the individual directly due to the risk the individual would face from his country's own internal security service. Intelligence reporting showed that the individual was in contact with another person that the UK agencies might be able to approach with lower risk. The reporting, however, did not fully identify who this contact was. The security and intelligence agencies used BPD to identify that contact conclusively, enabling them to determine that they could safely approach the contact and seek support. The contact has been successfully recruited as an agent to help collect intelligence and protect the UK's national security.

Protection of major events

When significant events take place – such as the NATO Summit in Wales in 2014 or the London Olympics in 2012 – the security and intelligence agencies work to ensure they occur safely. This includes tracing the details of individuals with access to venues so as to mitigate the risk that subjects of national security interest might gain access to these events. The majority of individuals in such datasets will not be of direct intelligence interest and this data is therefore treated as BPD. Without using this information, it would be far harder, more costly and intrusive for the police and agencies to put in place alternative measures to provide security assurance.