RUSI
www.rusi.org

Royal United Services Institute
for Defence and Security Studies

Briefing Paper, November 2015

Understanding the Investigatory Powers Bill

Calum Jeffray

Key Points

- Many of the most significant proposed changes to the existing framework for investigatory powers available to the government relate not to the powers themselves, but to the authorisation and oversight mechanisms that govern them
- The draft legislation makes explicit a number of capabilities that until now were lawful under very broad, general powers
- The draft bill sets out the extent of bulk capabilities currently used by agencies, some of which have only recently been fully avowed
- Much of the early criticism of the draft bill targets the proposed obligation on communications service providers to retain a type of communications data known as internet connection records.

ON 4 November the government published the draft Investigatory Powers Bill, set to be one of the most ambitious pieces of legislation laid before this Parliament. For some, the proposed bill is 'neither a snooper's charter nor a plan for mass surveillance',[1] but a welcome update to laws that have not kept pace with technological change, which will allow the police and intelligence agencies to operate effectively in a digital age. For others, the bill constitutes a 'breath-taking attack on the internet security of every man, woman and child' in the UK, and is an attempt by the state to 'grab even more intrusive surveillance powers' to spy on its citizens.[2] The draft bill goes into an unprecedented level of detail on the powers available to the government, and significantly increases the extent of legal safeguards and judicial oversight. It is now for politicians and the public to decide whether the right balance has been struck.

1. As observed by the shadow home secretary following the bill's unveiling in Parliament. See *BBC News*, 'Details of UK Website Visits "To Be Stored for Year"', 4 November 2015.
2. Don't Spy on Us, 'Don't Spy on Us Response to the Investigatory Powers Bill', <https://www.dontspyonus.org.uk/blog/2015/11/04/dont-spy-on-us-response-to-the-draft-investigatory-powers-bill/>, accessed 6 November 2015.

Given the technical and legal complexities of the subject matter, the draft bill is a lengthy document, totalling 299 pages including explanatory notes. This guide is designed to provide an overview of the proposed legislation, the main powers and safeguards it contains, and topics for debate.

Context

The Investigatory Powers Bill featured in the Queen's Speech of May 2015 and has been foreseen since the introduction of the Data Retention and Investigatory Powers Act (DRIPA) 2014. Providing time to consult on and develop a new legal framework, DRIPA 2014 included a sunset clause which meant that it would have to be replaced by primary legislation by 31 December 2016.[3] Meanwhile, three independent reports were prepared to inform the government's policy: the Intelligence and Security Committee's (ISC) report on privacy and security, published in March 2015; David Anderson QC's Investigatory Powers Review (IPR), published in June 2015; and the Independent Surveillance Review (ISR) of the Royal United Services Institute (RUSI), published in July 2015.[4] The draft bill draws heavily on the 198 recommendations made by the three independent reviews. Their conclusions echoed public calls for reform to the legislation governing the collection, retention, and use of data and communications for intelligence-gathering and law-enforcement purposes.

Towards a Clearer and More Comprehensible Framework

There is near-consensus in public opinion that there are circumstances in which law-enforcement agencies (LEAs) and security and intelligence agencies (SIAs) require sensitive capabilities to obtain communications in order to safeguard national security, investigate crimes and protect the public. The agencies maintain that they require appropriate powers to adapt to the current digital age; the current pace of technological change is unprecedented, and the rapid uptake of mobile phones, portable computers and handheld devices has both enabled access to the Internet on the go and transformed the

Key Terms

Interception: the ability to acquire the content of communications (for example, the body of an e-mail, or what was said during a telephone conversation).

Communications data: information relating to a piece of communication (for example, relating to an e-mail: the sender, recipient, time and date it was sent).

Equipment interference: accessing computer equipment to acquire private data, including communications (also known as computer network exploitation or hacking).

3. In July 2015, a legal challenge by David Davis MP and Tom Watson MP was upheld by the High Court, which ruled that aspects of DRIPA 2014 were unlawful and should be disapplied after 31 March 2016. The Home Office appealed the ruling, though the Court of Appeal has not yet expressed a view on the status of DRIPA 2014 between April and December 2016.
4. Sir Nigel Sheinwald was also tasked to review work with governments and communications service providers (CSPs) overseas in order to improve access to data across different jurisdictions for intelligence and law-enforcement purposes.

way in which we all communicate.[5] This includes the small minority of terrorists, criminals, their victims, missing persons, and others to whose data and communications the agencies require access. At the same time, concerns have been raised over the lawful extent of these agencies' powers, how they are used, and the degree to which the communications of ordinary citizens are affected by the activities of the agencies.

The reviews found that the existing laws in this area are neither coherent nor comprehensible, especially the Regulation of Investigatory Powers Act (RIPA) 2000,[6] and safeguards and oversight mechanisms are insufficient to inspire public confidence.[7] As a result, members of the public are unsure of how they are affected by data collection, the purpose for which data are collected, and what checks and balances are in place to ensure that the intrusive powers granted to LEAs and SIAs are not misused. This was particularly apparent in the wake of the disclosures made by former National Security Agency contractor Edward Snowden in 2013, which seemed to suggest that the UK and US governments were conducting mass surveillance of their citizens. Any new legislation, the reports concluded, therefore needed to be clearer and enhance independent oversight in order to regain public trust.

The proposed Investigatory Powers Bill is designed to provide the statutory basis for all powers available to the authorities to collect electronic communications, including the ways in which these are authorised and overseen. The process for granting warrants for the use of these powers introduces a 'double lock' of consent – authorisation by the secretary of state followed by judicial approval – before the warrant can enter into effect. The draft bill provides additional safeguards relating to sensitive professions such as lawyers, journalists and MPs (whose communications could only be intercepted following authorisation from the prime minister). Finally, the draft bill strengthens oversight arrangements by establishing the position of an independent Investigatory Powers Commissioner (IPC) who, together with judicial commissioners and legal and technical experts, would authorise and oversee the use of all of the powers under the draft bill.

Some of the capabilities granted under these powers are well known; others were only recently explicitly avowed in public, including the ability of SIAs to hack into phones and other devices. The powers contained in the draft bill are divided into three categories: acquiring the content of communications (interception); accessing communications data; and equipment interference (EI). A consistent distinction is made between the use of these powers for targeted and bulk purposes. Few changes have been made to interception powers under the current framework, while the most noticeable legislative change relates to EI, and is likely to remain controversial. Changes have also been made to the way in which communications data are classified, with critics of the draft bill most concerned over the one new proposed power: the obligation for communications service providers (CSPs) to log and retain a type of communications data

5. 'A Democratic Licence to Operate: Report of the Independent Surveillance Review', *Whitehall Report 2-15*, RUSI, London, July 2015, p. 5.
6. David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (London: The Stationery Office, 2015), p. 8.
7. 'A Democratic Licence to Operate', p. 82.

known as internet connection records (ICRs), which is a record of the interactions between an individual's device (for instance, a mobile phone or laptop) and the Internet.

Authorisation and Oversight

The draft bill creates a new process for signing off warrants, which, except in one instance, must be both authorised by the secretary of state and approved by a judicial commissioner before implementation. An independent Investigatory Powers Commissioner would also be established, with responsibility for both authorisation and oversight of the powers outlined in the bill. The commissioner would be able to draw on greater technical and legal expertise, and would benefit from a more visible profile when engaging with industry, Parliament and the public. The draft bill also establishes a domestic right of appeal to judgments made by the Investigatory Powers Tribunal (IPT).

Many of the most significant changes to the existing framework relate not to the powers themselves, but to the authorisation and oversight mechanisms which govern them. In this regard, the ISR was particularly influential in proposing a dual authorisation process and unified judicial oversight body.

One of the most contentious issues over investigatory powers has been whether it is more appropriate for government ministers or judges to authorise warrants for their use. In summary, these arguments tend to relate to issues of trust (judges would bring independent assessment to the decision-making process and are thought to inspire greater public confidence than ministers), capability (the extent to which each party is qualified to make legal judgments and/or judgements over political risk) and accountability (ministers are accountable to Parliament for their decisions, whereas a right of appeal exists for those dissatisfied with a judicial decision).[8] The draft bill takes into account the recommendations of the IPR and ISR in proposing a regime in which all warrants (whether for the purposes of national security or serious crime, related to interception, communications data or EI, or related to targeted or bulk powers) would be subject to the 'double lock' of authorisation by the secretary of state and approval by a judicial commissioner before implementation.[9] In urgent situations, such as when lives are endangered, the secretary of state would have the power to approve a warrant that would come into immediate effect, with judicial review carried out within five days. In any case, the decision of the judicial commissioner would be final.

Under the current legal framework, oversight of the LEAs and SIAs is conducted by a number of bodies, whether executive (the home secretary, responsible for LEAs and MI5, and foreign secretary, responsible for SIS and GCHQ), parliamentary (through the ISC) and judicial (through a number of judicial commissioners with specific areas of responsibility, and the IPT). All three independent reviews recommended strengthening oversight mechanisms, on the basis that

8. *Ibid*., p. 110.
9. The one exception is an EI warrant sought by LEAs, which would be authorised by a chief constable rather than a secretary of state, and approved by a judicial commissioner before implementation.

the public has limited knowledge and understanding of how the current arrangements work.[10] Criticisms include the fact that there is little clarity on the demarcation between some oversight bodies, many do not have a sufficiently public-facing profile, and some only have a remit to conduct narrow rather than comprehensive investigations into agencies' activities.

Following the recommendations of both the IPR and ISR, the draft bill proposes a radical overhaul of oversight arrangements in establishing the IPC. The IPC's office would merge the offices of the Interception of Communications, Surveillance and Intelligence Services Commissioners, and would have a number of additional functions. It would house the judicial commissioners authorising and reviewing warrants and their application; have access to technical and legal expertise to conduct in-depth reviews of the agencies and their work; and have a public-facing profile, publishing statistics, annual reports and guidance on interception, communications data and EI powers.

The IPC would also have the authority to inform individuals that they had been subject to errors by LEAs and SIAs, enabling them to take a case to the IPT. Responding to recommendations in all three independent reviews, the draft bill provides for a domestic right of appeal to rulings by the IPT (until now, appeal cases could only be heard by European courts). The bill does not propose changes to the ISC or its oversight role.

The Proposed Powers

Interception

The draft bill brings together the existing interception powers under RIPA 2000 and the Wireless Telegraphy Act (WTA) 2006. Little has changed in terms of the agencies that can seek warrants to intercept *targeted* communications, or the purposes for which this power can be used. However, only the SIAs would be able to seek *bulk* interception warrants, and only for the purpose of national security. All warrants would be authorised by a secretary of state, subject to judicial approval before the warrant comes into force.

Interception powers relate to the ability of LEAs and SIAs to collect the *content* of communications in the course of transmission or while on a server, for example. In 2014, 2,795 interception warrants were issued, of which 68 per cent related to serious crime, 31 per cent to national security and 1 per cent to a combination of the two.[11] The bill seeks to replace the existing interception powers under Chapter I of RIPA 2000, as well as Section 49 of the WTA 2006 (the IPR found that there is 'no operational distinction between the two statutes').[12]

In order to obtain a warrant authorising interception, the agency in question must demonstrate that such interference with an individual's privacy is both necessary (whether in the interests of

10. 'A Democratic Licence to Operate', p. xii.
11. Anthony May, *Report of the Interception of Communications Commissioner: March 2015*, HC 1113 (London: The Stationery Office, 2015), pp. 27–28.
12. Anderson, *A Question of Trust*, p. 97.

national security, for the purpose of preventing or detecting serious crime, or in safeguarding the economic wellbeing of the UK) and proportionate (that is, the intrusion is reasonable, in accordance with the intelligence requirement). The ability to apply for a warrant is limited to nine agencies: MI5; SIS; GCHQ; the National Crime Agency; the Metropolitan Police; the Police Service of Northern Ireland; Police Scotland; HM Revenue and Customs; and the Ministry of Defence (MoD). All of these measures would remain unchanged in the proposed legislation.

Targeted interception powers currently exist under Section 8(1) of RIPA 2000, applicable to 'one person as the interception subject' or 'a single set of premises'.[13] However, the law has been criticised for being insufficiently clear, given that the stated definition of 'person' includes 'any organisation and any association or combination of persons'.[14] The proposed bill explicitly notes that applications for targeted interception warrants would need to specify a particular person, premises or operation.

The interception of communications in bulk has proved to be a contentious issue given the potential volume of communications affected, leading to accusations of 'mass surveillance'. Warrants under RIPA 2000 Section 8(4) are currently used to intercept communications traffic carried by fibre-optic cables, rather than the communications of a specific individual. They apply to external communications, where the sender and/or the recipient must be located outside the British Islands. All three reviews concluded that bulk interception does not equate to mass surveillance, but that the nature and lawful extent of this collection should be set out much more clearly in statute. The draft bill proposes a bulk interception warrant, which could only be sought by the SIAs to acquire intelligence relating to individuals outside the UK for the purpose of national security. Once the data have been intercepted, an additional warrant, detailing a specific operational purpose, would be required to access any data relating to persons in the UK. Warrants for both targeted and bulk interception would have to demonstrate necessity and proportionality, and would require authorisation by a secretary of state and approval by a judicial commissioner before being implemented. The IPC would oversee the use of interception powers and ensure that warrants are compliant with legislation.

Communications Data

The draft bill replaces provisions relating to communications data in RIPA 2000, the Anti-Terrorism, Crime and Security Act 2001, DRIPA 2014, and the Counter-Terrorism and Security Act (CTSA) 2015. Existing categories (traffic data, service-use information and subscriber information) would be replaced by entity data (relating to people or objects) and event data (things that have happened). CSPs would be required to retain communications data for up to twelve months, including ICRs, with access to be authorised by two senior officers within each agency (as is current practice). If an agency seeks to obtain communications data in bulk, a warrant would be required, authorised by the secretary of state and approved by a judicial commissioner.

An important premise of existing legislation is that access to communications data is less intrusive to an individual's privacy than intercepting the content of his or her communications.

13. Regulation of Investigatory Powers Act (RIPA) 2000, Section 8(1).
14. RIPA 2000, Section 81.

This has not been without challenge, however, and a number of aspects of the rules governing access to communications data remain contentious. For example, the list of bodies granted use of this capability is longer than for interception (and includes local authorities); there is a greater range of purposes for which data can be sought (for instance, public safety, health, preventing death or injury in an emergency); and the authority to issue a notice to CSPs for data resides internally with a Designated Person (a senior official within the organisation in question but independent of the investigation to which the data relate). All three independent reviews agreed that communications data have become an essential investigative tool for LEAs in particular. There were 517,236 notices and authorisations issued in 2014, of which 88.9 per cent were issued by LEAs, 9.8 per cent by SIAs and 1.3 per cent by local and other public authorities.[15]

The draft bill maintains the principle that access to communications data is less intrusive than interception of the communications' content, and provides new definitions of content and communications data. It also proposes two new categories of communications data to replace the existing categories. Previously, such data were classified as traffic data (data attached to a communication, such as sender, recipient and time/location of transmission); service-use information (data relating to a person's use of a communications service); and subscriber information (data held or obtained by a CSP on a customer). The bill proposes two categories: 'entity data' – information about people and devices, which is considered less intrusive; and 'event data' – information on interactions and things that have happened, considered more intrusive.

Until recently, CSPs were obliged to retain only data that they generate or process in the UK in the course of providing their service. The bill conserves the provisions of CTSA 2015 which, for the first time, required CSPs to retain communications data necessary to enable authorities to resolve IP addresses.[16] The one new power under the draft bill would further oblige CSPs to retain ICRs. This would include, for example, websites, applications and services accessed by the device (such as BBC News, Google or Facebook), but not the specific pages visited or the information accessed (specific news articles, web searches or profile pages). The government argues that, in practice, this new power would only be used in three circumstances: to identify the sender of a communication online; to establish what communications services a known victim or suspect used; to establish whether a known suspect has been involved in online criminality (for example, accessing child pornography websites or terrorist material). Only certain agencies would be able to request ICRs (with the notable exclusion of local authorities). Nevertheless, opponents argue that forcing CSPs to record the internet activity of everyone in the UK is an unnecessary privacy intrusion, with the retention of such data making it vulnerable to hackers and breaches, such as that experienced by TalkTalk in October 2015.

15. May, *Report of the Interception of Communications Commissioner: March 2015*, pp. 48–49.
16. IP (Internet Protocol) addresses are assigned by CSPs to devices each time they connect to the Internet. IP address resolution is the process of identifying which device used an IP address at a given point in time, which can then be used to identify who has accessed a particular service or website.

Under the draft bill, CSPs would continue to be obliged to retain communications data, now also including ICRs, for a period of up to twelve months, and to hand the data over to public authorities when requested. Those authorities able to make such requests and the types of data they have access to will be continually reviewed (the draft bill proposes a total of forty-two LEAs and public authorities in addition to the SIAs and MoD). As is the case currently, only a Designated Person would be able to authorise a request for data held by CSPs, after consulting another official within the organisation known as the Single Point of Contact (an individual certified to facilitate lawful acquisition of communications data).

The existing ability to require CSPs to supply communications data in bulk was avowed by Theresa May in introducing the draft bill. The home secretary referred to Section 94 of the Telecommunications Act 1984, under which she said successive governments had allowed all three SIAs to access phone communications data in bulk, typically to identify networks at pace by tracking calls made from a suspicious number (the SIAs would see details of calls, but not the content).[17] According to David Anderson, 'It wasn't illegal in the sense that it was outside the law, it was just that the law was so broad and the information was so slight that nobody knew it was happening'.[18] Section 94 would be abolished under the new legislation, to be replaced by a bulk communications data warrant, which only the SIAs would be able to seek for the purpose of national security (and which could not authorise the collection or examination of the content of communications). Access to data would be granted only if deemed necessary and proportionate for one or more operational purposes, with the warrant authorised by a secretary of state and approved by a judicial commissioner before being implemented. The IPC would oversee the use of all communications data powers and ensure that warrants are compliant with legislation.

Equipment Interference

The bill makes the implicit powers regarding EI contained in existing legislation explicit, placing it on a clearer statutory footing. The bill introduces authorisation levels, statutory purposes, safeguards and oversight measures consistent with the interception regime.

The Intelligence Services Act (ISA) 1994 gives the relevant secretary of state the power to issue warrants authorising the SIAs to interfere with property and wireless telegraphy, broadly defined. In February 2015, the publication of the draft Equipment Interference Code of Practice made clear that the government considers 'property' to include equipment, which may encompass, but is not limited to, 'computers, servers, routers, laptops, mobile phone and other devices'.[19] To date, the lack of a clear and explicit basis in legislation for EI by the SIAs, other than general powers set out in the ISA 1994, has attracted criticism. Liberty, for example, accused the

17. Gordon Corera, 'How and Why MI5 Kept Phone Data Spy Programme Secret', *BBC News*, 5 November 2015.
18. *BBC News*, 'MI5 "Secretly Collected Phone Data" for Decade', 5 November 2015.
19. Home Office, 'Equipment Interference: Code of Practice', draft for public consultation, February 2015, p. 5, footnote 6.

government of trying to 'effectively legislate for [EI] via a Code of Practice'.[20] The absence of effective oversight of these activities was also noted by the IPR, which suggested that the 'lack of clear statutory authority for such powers insulates them from public-facing oversight'.[21]

The more explicit statutory footing for EI is among the controversial aspects of the proposed bill. The IPR noted that this capability 'presents a dizzying array of possibilities to the security and intelligence agencies', and acknowledged that 'while some methods of [EI] may be appropriate, many are of the view that there are others which are so intrusive that they would require exceptional safeguards for their use to be legal'.[22]

There are notable similarities between interception and EI, which both seek to access content data, albeit via different means. As such, the measures governing EI powers set out in the draft bill reflect the interception regime; for instance, the ability of an agency to apply for a warrant would be limited to the same purposes (although LEAs would only be able to apply for an EI warrant for the purposes of preventing and detecting serious crime). There would be an explicit obligation on CSPs to assist in giving effect to those EI warrants served by the SIAs.

There are also provisions in the new bill to allow bulk EI. The draft bill proposes a bulk EI warrant which could only be sought by the SIAs, in order to acquire intelligence relating to individuals outside the UK for the purpose of national security. Once the data has been acquired an additional warrant, detailing the specific operational purpose, would be required to access any content data relating to persons in the UK. Warrants for both targeted and bulk EI would have to demonstrate necessity and proportionality, and would need to be authorised by a secretary of state (or chief constable for LEAs) and approved by a judicial commissioner before being implemented. The IPC would oversee the use of EI powers and ensure that warrants are compliant with legislation.

Bulk Powers in the Spotlight

The bill brings together all of the bulk intelligence-gathering powers available to the SIAs. New safeguards, authorisation and oversight measures have been proposed that specifically relate to bulk powers.

In addition to using their capabilities to target particular individuals of interest, the SIAs make use of a range of bulk powers. These are most frequently used for the purposes of overseas 'target discovery': to detect, identify, to develop intelligence on new or possible threats outside of the UK.[23] Bulk access capabilities have been highlighted by SIAs as critical to providing information on cyber-security threats. David Anderson found that his investigations left him in 'not the slightest doubt that bulk interception, as it is currently practised, has a valuable

20. Liberty, 'Liberty's Response to the Home Office Consultation on the Equipment Interference Code of Practice', March 2015, p. 10.
21. Anderson, *A Question of Trust*, p. 215.
22. *Ibid*., p. 227.
23. 'A Democratic Licence to Operate', p. 18.

role to play in protecting national security'.[24] The IPR and ISR argued for bulk capabilities to be maintained where the operational and legal case for necessity and proportionality is made.

Until now, there has been an overall lack of legislative clarity around bulk capabilities. A warrant under RIPA 2000 Section 8(4) is targeted at a telecommunications system and therefore, in effect, targets communications bearers rather than specific, individual communications. However, it is not explicitly described as a mechanism for bulk data collection, though in practice this is one of its most common uses. This lack of clarity has raised questions as to whether such collection occurs in accordance with the law, particularly as the nature of bulk data collection was hitherto largely unknown. Privacy campaigners assert that these powers are not a proportionate or necessary intrusion into a citizen's privacy and as such are in breach of the rights guaranteed under European law. The issue of whether bulk collection is necessary and proportionate under Article 8 of the European Convention on Human Rights (the right to privacy) is currently under review by the European Court of Human Rights.

As noted in the sections above, the draft bill makes a consistent distinction between targeted and bulk powers in relation to the three categories of capabilities (interception, communications data and EI). The IPR stressed that powers relating to bulk data and bulk interception should be subject to separate authorisation and oversight mechanisms, and limited to specific agencies. This is reflected in the draft bill; only the SIAs are able to seek bulk warrants of any kind, only for the statutory purpose of national security, and only once an operational purpose for the warrant has been provided. As with targeted warrants, bulk warrants must be authorised both by the secretary of state and approved by a judicial commissioner.

Bulk Personal Datasets

Bulk Personal Datasets (BPDs) are databases containing information on a large number of people (examples include telephone directories, electoral rolls and land registries). The use of BPDs by the intelligence agencies was avowed for the first time by the ISC in March 2015, though the Security Service Act 1989 and ISA 1994 allow the SIAs to conduct intelligence and security operations which, the agencies have argued, extend to examining datasets. Following criticism that, again, this capability was not sufficiently clear in statute, the draft bill mandates that a warrant must be granted for SIAs to obtain, retain or examine a BPD. There is also provision for the SIAs to seek a warrant for 'classes', or categories, of BPDs such as travel data (although the term 'classes' is not explicitly defined). Warrants would need to be authorised by a secretary of state and approved by a judicial commissioner before being implemented. The IPC would oversee use of BPDs and ensure warrants are compliant with legislation.

A National Bill in an International Context

There are a number of challenges which continue to loom large for the government, especially at the international level. Perhaps the most striking of these is encryption. While encryption is recognised (including by the government) as critical to enhancing cyber-security to protect the

24. Anderson, *A Question of Trust*, p. 130.

communications and data of citizens and companies, the challenge for LEAs and SIAs is that the encrypted devices and communications of criminals, terrorists and other nefarious actors cannot easily be accessed or monitored, even pursuant to a lawful investigation.[25] A speech by Prime Minister David Cameron in January 2015 following the terrorist attacks in Paris, in which he suggested that there should be no 'means of communication' which 'we cannot read',[26] added to fears arising from the Snowden revelations that public authorities were seeking to break encryption standards. However, given the speed with which encryption technology is developing, and lack of agreement on the part of technology companies based in foreign jurisdictions such as the US, it seems there is little the government can do in legislative terms in response to encryption technology.

The lack of international agreement is also evident in the absence of measures in the draft bill relating to the work of Sir Nigel Sheinwald, and particularly to mutual legal assistance treaties and the sharing of intelligence material with foreign governments. The government remains committed to establishing an interstate agreement on lawful data-sharing between jurisdictions but until such an agreement is reached, the status quo looks set to continue.

A New Licence to Operate?

There is agreement on all sides that a new law is needed, and the government has done what was recommended by the three independent reviews in terms of clearly setting out the lawful extent of the most intrusive capabilities of the LEAs and SIAs.

The Investigatory Powers Bill currently remains in draft form. The bill will be subject to a period of public consultation and pre-legislative scrutiny by a dedicated joint committee of both Houses of Parliament. The joint committee will recommend any changes in a report published early in the new year. According to the standard passage of a bill through Parliament, the revised and updated bill (expected in early 2016) will then be subject to three readings in each House before the final bill can receive royal assent.

The degree of both public and parliamentary scrutiny will be unprecedented, and as the draft bill is debated, there will undoubtedly be disagreement over whether certain proposed powers go too far and whether safeguards go far enough. Earlier this year, RUSI's ISR panel called for consensus on a democratic licence for the agencies to operate. With more information available than ever before to inform the debate, the decision on whether the Investigatory Powers Bill is an appropriate piece of legislation will at least be a democratic one.

Calum Jeffray is a Research Fellow within the National Security and Resilience studies group at RUSI. He conducts research and analysis on a number of subject areas including cyber-security, intelligence, counter-terrorism and organised crime. He was part of RUSI's secretariat to the Independent Surveillance Review.

25. 'A Democratic Licence to Operate', p. 13.
26. *BBC News*, 'David Cameron Says New Online Data Laws Needed', 12 January 2015.

Royal United Services Institute
for Defence and Security Studies

Over 180 years of independent defence and security thinking

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

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

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

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

RUSI is a registered charity (No. 210639)