Bloomberg Law

Privacy and Security Law Report®

U.K. Investigatory Powers Act

The landmark U.K. Investigatory Powers Act governs the powers available to the police, security and intelligence agencies to gather and access electronic communications, but ongoing litigation ensures that there is more to come in this saga at least as long as the U.K. remains part of the European Union, the authors write.

The New U.K. Investigatory Powers Act—Under The Spotlight Following Key EU Ruling

BY RAFI AZIM-KHAN AND STEVEN FARMER

On Nov. 29, 2016, the Investigatory Powers Bill received Royal Assent to become the Investigatory Powers Act 2016. The Bill, which the Government called a ''landmark bill,'' sets out and governs the powers available to the police, security and intelligence agencies to gather and access electronic communications. The Government says that the 2016 Act will ''ensure that law enforcement and the security and intelligence agencies have the powers they need in a digital age to disrupt terrorist attacks, subject to strict safeguards and world-leading oversight.'' The Government also says that the new legislation brings together and updates existing powers while radically overhauling how they are authorised and overseen. In the Government's view, the new Act protects both the privacy and security of the public by introducing a ''double-lock'' for the most intrusive powers, so that warrants issued by a secretary of state will also require the approval of a senior judge, and by the introduction of an Investigatory Powers Commissioner (IPC) to oversee how the powers are used. There are also new protections for journalistic and legally privileged material and a requirement for judicial authorisation for the acquisition of communications data that identify journalists' sources. The Act also now contains sanctions, including the creation of new criminal offences, for those misusing the powers. However, to complicate matters, on Dec. 21, 2016, the Court of Justice of the European Union (CJEU) ruled, in Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C 698/15 Secretary of State for the Home Department v Tom Watson, that Members States cannot impose a general obligation to retain data on providers of electronic communications services.

Rafi Azim-Khan is a partner at Pillsbury Winthrop Shaw Pittman LLP, London and is head of the firm's data privacy practice group.

Steven Farmer is counsel at Pillsbury Winthrop, London and member of the firm's data privacy practice group.

Background

On March 1, 2016, the Government introduced a revised Investigatory Powers Bill to Parliament, amidst continued criticism from industry. Six draft Codes of Practice were also published alongside the Bill (see The Reporter 111[35]).

The revised Bill replaced the Bill the Government originally introduced in November 2015 (see The Reporter 108[28]). The Government said that the revised Bill responded to the concerns raised by three Parliamentary committees (the Joint Committee, the Intelli-

gence and Security Committee and the Science and Technology Committee) all of which had scrutinised the Government's original proposals.

The Bill, which has now received Royal Assent, consolidates existing legislation on the state's ability to access communications data. It repeals and replaces part 1 of the Regulation of Investigatory Powers Act 2000 (RIPA). It also replaces the emergency legislation passed in July 2014, i.e. the controversial Data Retention and Investigatory Powers Act 2014 (DRIPA), which expired on Dec. 31, 2016 (see The Reporter 95[27]). DRIPA was introduced in response to the CJEU's judgment of April 8, 2014 in Joined Cases C-293/12 Digital Rights Ireland (see The Reporter 92[110]), which declared the Data Retention Directive (2006/24/EC) invalid.

Legislative Scrutiny

Over 1,700 proposed amendments to the revised Bill were debated by Parliament before it concluded its passage on Nov. 16, 2016.

During its passage through the House of Commons, a number of Government amendments were made to the Bill in response to concerns raised by the Opposition and others. These included overarching provisions making explicit the privacy protections which run throughout the Bill; further enhancements to safeguards, such as those which apply to the modification process for warrants; and changes to the warrant and notice serving procedure to provide greater reassurance to communications service providers.

Other amendments included enhanced protections for sensitive professions and parliamentarians, including the requirement that a Judicial Commissioner must consider that there is ''an overriding public interest'' before any request to identify a journalist's source can be approved. The Prime Minister must also personally approve a warrant to obtain the communications of an MP or a member of another relevant legislature.

The Bill was introduced in the House of Lords on June 8, 2016. A number of Government amendments were made at the Report stage, with a particular focus on protections for legally privileged material and journalistic sources and material, and stronger safeguards for retention of communications data.

The Intelligence and Security Committee successfully tabled amendments to create an offence for the misuse of bulk powers, and to provide the Committee with access to the results of investigations carried out by the IPC on the basis of a referral from the Committee, insofar as they relate to the Committee's functions.

The Government also accepted an Opposition amendment requiring that access to internet connection records for the purpose of preventing or detecting crime should only be permitted, subject to limited exceptions, for the investigation of offences carrying a maximum sentence of at least 12 months.

Summary of the Act

According to the Explanatory Memorandum, the Act provides an updated framework for the use (by the security and intelligence agencies, law enforcement and other public authorities) of investigatory powers to obtain communications and communications data. These powers cover (i) the interception of communications; (ii) the retention and acquisition of communications data; and (iii) equipment interference for obtaining communications and other data. It is not lawful to exercise such powers other than as provided for by the Act. The Act also makes provision relating to the security and intelligence agencies' retention and examination of bulk personal datasets.

The Intelligence and Security Committee successfully tabled amendments to create an offence for the misuse of bulk powers.

The Act governs the powers available to the state to obtain communications and communications data. It provides consistent statutory safeguards and clarifies which powers different public authorities can use and for what purposes. It sets out the statutory tests that must be met before a power may be used and the authorisation regime for each investigative tool, including a new requirement for Judicial Commissioners to approve the issuing of warrants for the most sensitive and intrusive powers.

The Act also creates a new Investigatory Powers Commissioner to oversee the use of these powers. Finally, the Act provides a new power for the Secretary of State to require, by notice, communications services providers to retain internet connection records.

Part 1: General Privacy Protections

Section 2 of the Act sets out the numerous duties and considerations to which public authorities must have regard when taking decisions regarding the exercise of functions under the Act, including whether to issue warrants, grant authorisations or give notices.

When taking such decisions the public authority must consider whether what is sought to be achieved could reasonably be achieved by less intrusive means. The public authority must also have regard to the public interest in the protection of privacy and the integrity and security of telecommunication systems and any other aspect of the public interest in the protection of privacy.

Section 3(1) makes it an offence to intentionally intercept a communication in the course of its transmission without lawful authority. This applies to communications in the course of transmission via a public telecommunications system, a private telecommunications system or a public postal service. This offence previously existed under RIPA.

Where unlawful interception has taken place, but the person responsible was not intending to intercept a communication, the IPC may impose a fine.

Section 11 creates the offence of knowingly or recklessly obtaining communications data from a telecommunications or postal operator without lawful authority. It is a defence if it can be shown that the person acted in the reasonable belief that they had lawful authority to obtain the communications data.

  PVLR ISSN 1538-3423

Part 2: Lawful Interception of Communications

Warrants Chapter 1 covers interception and examination with a warrant. There are three types of warrants that can be issued:

- (i) targeted interception warrant: authorises any activity for obtaining secondary data;

- (ii) targeted examination warrant: authorises the examination of material that has been collected under a bulk interception warrant and must be sought whenever the intelligence service wishes to look at material relating to a person in the U.K. and it is necessary and proportionate to select the content of that person's communications for examination; and

- (iii) mutual assistance warrant: gives effect to an incoming request or authorises an outgoing request for assistance in relation to the interception of communications.

Those who may apply to the Secretary of State for an interception warrant are the heads of: (i) the three intelligence agencies; (ii) the National Crime Agency (NCA); (iii) the Metropolitan Police; (iv) the Police Services of Northern Ireland and Scotland; (v) HM Revenue & Customs; and (vi) the Chief of Defence Intelligence. A competent authority of another country may also apply for a mutual assistance warrant.

Power to Issue a Warrant Section 19 provides that the Secretary of State has power to issue a warrant if he/she considers that it is necessary:

- (i) in the interests of national security;

- (ii) for the purpose of preventing or detecting serious crime;

- (iii) in the interests of the economic well-being of the U.K. (in circumstances relevant to the interests of national security); or

- (iv) for giving effect to the provisions of a mutual assistance agreement.

The Secretary of State must also consider it to be proportionate to what is sought to be achieved. The decision of the Secretary of State to issue the warrant must then be approved by a Judicial Commissioner before the warrant can be issued.

Sections 20(5) and (6) provide that a warrant cannot be considered necessary if its only purpose is gathering evidence for use in legal proceedings, or only on the basis that the information that would be obtained relates to trade union activity in the U.K.

Section 23 provides that the Judicial Commissioner must, when considering whether to approve the issue of a warrant or not, review the conclusions the Secretary of State came to regarding the necessity and proportionality of the warrant and apply the same principles that a court would apply on an application for judicial review.

However, if the Secretary of State deems the warrant to be urgent then it can be issued without the approval of a Judicial Commissioner. A Judicial Commissioner must be notified that the urgent warrant has been issued and he/she must then decide whether to approve the decision or not within three working days.

If the Judicial Commissioner refuses to approve the urgent warrant then it ceases to have effect and cannot be renewed.

Safeguards The Act includes safeguards where the material concerned is legally privileged, contains confidential journalistic material or would identify a journalistic source.

For legally privileged material, the person issuing the warrant must consider the public interest in the confidentiality of items subject to privilege and must be satisfied that there are exceptional and compelling circumstances that make the interception or selection for examination of these items necessary. They must also be satisfied that there are specific arrangements in place for how these items will be handled, retained, used and destroyed.

As for confidential journalistic material and journalist sources, specific arrangements must be in place for the handling, retention, use and destruction of such material.

Other Forms of Lawful Interception Chapter 2 deals with other forms of lawful interception (such as interception with consent and interception by businesses for the purpose of monitoring and record-keeping).

Further Safeguards

Chapter 3 covers certain other provisions about interception, including additional safeguards relating to the retention and disclosure of intercepted material. The Chapter provides that the issuing authority must ensure that arrangements are in force for securing that certain requirements are met relating to retention and disclosure of material obtained under a warrant. The number of persons who see the material, the extent of disclosure and the number of copies made of any material must be to the minimum necessary for the authorised purposes.

Further, where the interception concerns legally privileged material, the IPC must be informed as soon as is reasonably practicable and he/she has the power to order that the material be destroyed, or to impose conditions as to the use or retention of that material. Further the IPC must consider that the public interest in retaining the items outweighs the public interest in the confidentiality of such items, and that retaining them is necessary in the interests of national security or for the purpose of preventing death or significant injury. If that test is not met, the IPC must exercise the power to order destructions or impose conditions. Even if the test is met, the IPC may still impose any conditions he/she thinks necessary to protect the public interest in the confidentiality of the items.

Part 3: Authorisations for Obtaining Communications Data

Section 61 provides the power for relevant public authorities to acquire communications data. Communications data is the ''who'', ''when'', ''where'' and ''how'' of a communication, but not its content. An authorisation can be granted where a designated senior officer in a relevant public authority is content that a request is necessary for one of the ten purposes set out in subsection (7) and proportionate to what is sought to be achieved. [28]

The ten purposes are:

- (i) in the interests of national security;
- (ii) preventing or detecting crime or of preventing disorder;
- (iii) in the interests of the economic well-being of the U.K. so far as those interests are also relevant to the interests of national security;
- (iv) in the interests of public safety;
- (v) for the purpose of protecting public health;
- (vi) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- (vii) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;
- (viii) to assist investigations into alleged miscarriages of justice;
- (ix) where a person (''P'') has died or is unable to identify themselves because of a physical or mental condition, to assist in identifying P, or to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition; or
- (x) for the purpose of exercising functions relating to the regulation of financial services and markets, or financial stability.

Section 62 provides restrictions concerning the acquisition of internet connection records retained by communications service providers in accordance with a notice given by the Secretary of State under s 87 of the Act (see Part 4 below). It requires one or more of three conditions, A, B and C below, to be satisfied before data which is, or can only be obtained by processing, an internet connection record can be obtained.

Condition A is that the data is necessary, for any of the ten purposes in s 61(7) (see above), to identify the sender of an online communication. An application for such data will often be for the purposes of IP address resolution to determine which individual carried out that action at that time.

Condition B is that the data is to be obtained for any of the statutory purposes other than the prevention or detection of crime, and the data is necessary to identify:

- (i) which communication services a person has been using, for example determining whether they are communicating through apps on their phone;
- (ii) where a person has accessed illegal content, for example an internet service hosting child abuse imagery; or
- (iii) which internet service is being used and when and how it is being used.

Condition C is that the data is to be obtained for the prevention or detection of crime and is necessary for the same three investigative purposes described in Condition B. However, the crime to be prevented or detected must be serious crime or other relevant crime (as defined).

Under section 75 local authorities can only obtain communications data if approved by a relevant judicial authority.

Further, under section 77 data requests made to identify a journalistic source must be approved by a Judicial Commissioner, unless it is an imminent threat to life situation. In reaching a decision, the Judicial Commissioner must have regard to both the public interest in protecting a source of journalistic information and the need for there to be an overriding public interest before approving an authorisation.

Part 4: Retention of Communications Data

Section 87 gives the Secretary of State the power to require telecommunications operators to retain communications data, where necessary and proportionate for one or more of the ten statutory purposes set out above for a maximum period of 12 months.

The power is exercised by the Secretary of State giving a retention notice to a telecommunications operator. The Secretary of State's decision must then be approved by a Judicial Commissioner.

A retention notice, which may relate to one or more operators, will require the retention of specified items of communications data for the period or periods set out in the notice, which must be no more than 12 months. The notice may also impose additional requirements and restrictions, such as requirements relating to the processing or security of retained data. Unless, or until, a retention notice is given, a telecommunications operator is not required to retain any communications data under this Act.

A retention notice cannot require the retention of so-called ''third party data.'' Where one telecommunications operator is able to see the communications data in relation to applications or services running over their network, but where they do not use or retain that data for any purpose, it is regarded as ''third party data.''

Communications data can be retained if it may be used to identify, or could assist in identifying, the sender or recipient of a communication (whether or not a person). Such communications data would include phone numbers, email addresses and source internet protocol addresses. Communications data that can be retained includes internet connection records.

Part 5: Equipment Interference

A targeted equipment interference warrant authorises the interference with equipment for the purpose of obtaining communications, information or equipment data.

This Part of the Act covers the Secretary of State's power to issue targeted equipment interference and targeted examination warrants and explains the activities and conduct that these warrants may authorise.

Part 6: Bulk Warrants

This part covers bulk interception warrants, bulk acquisition warrants and bulk equipment interference warrants.

The main purpose for which a bulk interception warrant can be issued is limited to intercepting overseas-related communications or obtaining secondary data from such communications. A bulk interception warrant cannot therefore be issued for the primary purpose

  PVLR ISSN 1538-3423

of obtaining communications between individuals in the U.K.

A bulk acquisition warrant authorises one or more of: (i) requiring a telecommunications operator to disclose specified communications data in its possession or to obtain and disclose communications data which is not in its possession; (ii) the selection for examination of the data obtained under the warrant; and (iii) the disclosure of data described in the warrant.

The main purpose for which a bulk equipment interference warrant may be issued is limited to interference with equipment to obtain overseas-related communications, overseas-related information or overseas-related equipment data. As with a bulk interception warrant, a bulk equipment interference warrant cannot be issued where the primary purpose is obtaining communications between individuals in the U.K.

The Government says that some of the provisions in the Act will require extensive testing and will not be in place for some time.

In all cases, the Secretary of State can issue a bulk warrant only where it is necessary and proportionate, for one or more specified statutory purposes. The interests of national security must always be one of those purposes. Further, the decision to issue the warrant must be approved by a Judicial Commissioner.

All bulk warrants (unless cancelled) last for six months from the date of issue or, in the case of a renewed warrant, from the day after it would otherwise have expired.

Safeguards are in place in respect of all bulk warrants in relation to the retention and disclosure of records and to the examination of data. Additional safeguards in relation to legally privileged material and confidential journalistic material are in place for bulk interception warrants and bulk equipment interference warrants.

For both types of warrants, when the use of certain criteria to select intercepted content for examination is either intended or likely to result in the acquisition of items subject to legal privilege, the use of those criteria must be approved by a senior official acting on behalf of the Secretary of State. That senior official may only give their approval if they are satisfied that there are exceptional and compelling circumstances which make the use of the criteria necessary, if the intention is specifically to acquire items subject to legal privilege, or, where the acquisition of such items is likely, specific arrangements are in place for how these items will be handled, retained, used and destroyed.

As for material containing confidential journalistic material, in the case of both bulk interception warrants and bulk equipment interference warrants, the IPC must be informed as soon as reasonably practicable.

In the case of all bulk warrants, it is a criminal offence to breach the safeguards relating to the examination of material.

Part 7: Bulk Personal Dataset Warrants

A bulk personal dataset is a set of information that includes personal data relating to a number of individuals, the majority of whom are not, and are unlikely to become, of interest to the service in the exercise of its functions. Section 199(1) sets out the circumstances in which an intelligence service retains a bulk personal dataset. Essentially, an intelligence service may not exercise a power to retain or examine a bulk personal dataset without a warrant.

As elsewhere in the Act, the Secretary of State cannot issue a warrant without approval by the Judicial Commissioner, unless the Secretary of State considers there is an urgent need to issue it, in which case the Judicial Commissioner must be informed of the issue and decide whether to approve the warrant or not within three days.

The Act contains additional safeguards for health records and legally privileged material.

Conclusion

The Government says that some of the provisions in the Act will require extensive testing and will not be in place for some time. The Home Office is developing plans for implementing the provisions in the Act and will set out the timetable in due course. The Government says that this will be subject to detailed consultation with industry and operational partners.

Comment

When the revised Investigatory Powers Bill was introduced to Parliament in March 2016, industry was still sceptical, with the Law Society saying that although it welcomed the acknowledgement of legal professional privilege in the draft Bill, it was concerned that the protection of the principle did not go far enough, and the News Media Association saying that it still did not include adequate safeguards to protect journalists' sources. Changes were made to the Bill to give greater protection to legally privileged material accidentally caught in a legitimate search ensuring its retention is subject to a public interest test, which satisfied the Law Society, but the newspaper industry is still not happy that journalists' sources are adequately protected.

In addition, the CJEU's decision in Home Office v Tom Watson (as mentioned above) further complicates matters. The CJEU found that EU law precludes a general and indiscriminate retention of traffic and location data, but that Member States can, if they wish, allow for the targeted retention of that data solely for the purpose of fighting serious crime, provided that such retention is, in terms of the kind of data retained, the means of communication in question, the people concerned and the duration of retention, limited to what is strictly necessary. Further, the CJEU said, access by national authorities to the retained data must be subject to conditions, including prior review by an independent authority and the data being retained within the EU.

Clearly, this decision affects the whole of Part 4 of the Act. In the CJEU's view, retained data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained. The fact that the data is retained without the users of electronic communica-

tions services being informed is, the CJEU says, ''likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance''.

Consequently, only the objective of fighting serious crime is capable of justifying such interference, the CJEU says. Legislation that prescribes a general and indiscriminate retention of data and does not require there to be any relationship between the retained data and any threat to public security and is not restricted to, for example, data pertaining to a particular time and/or geographical area and/or group of persons likely to be involved in a serious crime, exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society. The case will now return to the Court of Appeal who will interpret the CJEU's decision in the light of the 2016 Act. There is therefore more to come in this saga, at least in the medium term whilst the U.K. remains part of the EU.

  PVLR ISSN 1538-3423