DRAFT INVESTIGATORY POWERS BILL 2015

Date: 15 February 2016

Government Enforcement Alert

By: Christine Braamskamp, James G Millward, James G Millward

INTRODUCTION

On 4 November 2015 the Home Secretary published a Draft Investigatory Powers Bill (the "**Bill**"), emphasising its importance in combating the increasingly sophisticated communication technologies used by criminals to intercept, acquire and interfere with communications. Decried by its detractors as a "snooper's charter" but defended by its supporters as vital to tackling evolving cyber threats, the Bill is highly, and predictably, contentious. The Bill, which runs to 300 pages, has been published for pre-legislative scrutiny and public consultation and is intended to replace the emergency legislation passed in July 2014, the Data Retention and Investigatory Powers Act 2014 (**DRIPA**), which falls away on 31 December 2016. A joint committee (the "**Committee**") was set up to examine the Bill. The Committee published its report on 11 February 2016 and it will now be for the Government to respond.

SUMMARY

- The current powers to obtain communications and data about communications are contained within several pieces of legislation. The Bill purports to consolidate these powers and the safeguards that apply to them, and to place new powers of intrusive surveillance on a statutory footing.
- The Bill creates a new Investigatory Powers Commissioner (**IPC**) to oversee how these powers are used, abolishing and replacing the three different commissioners who have oversight currently.
- The Bill does not address the misalignment between the extent of the intercept powers proposed and the fact that intercept evidence remains inadmissible in the English courts. There is still no intention for intercept material to be used as evidence in the courts.
- Among the proposals is a provision to allow security agencies access to 'bulk data'. This would permit security agencies to trawl large pools of data that are "likely to include communications or other data relating to terrorists and serious criminals." Critics have suggested that this power is at odds with the traditional presumption that authority for targeted surveillance should only be granted where reasonable, prior suspicion is demonstrated.
- The Bill will allow the Home Secretary to issue a notice requiring a "telecommunications operator" to retain internet communications data for 12 months. This provision has caused alarm among corporates as the definition of "telecommunications operator" has been extended to refer to any company providing communications electronically.

- The Bill introduces a new "Equipment Interference" provision. The purpose of this provision is to authorise the subject of the Equipment Interference warrant, which is likely to be any company which controls electronic data, to access communications or other private information held on a computer. For many corporates, this raises the unsavoury prospect of assisting with the 'hacking' of their own customers' data.
- In its current form, the Bill provides limited protection for legal privilege. A Code of Practice setting out the position in relation to privilege is yet to be published.
- The Bill applies to the United Kingdom and is limited in jurisdiction. Notices and warrants authorised under the Bill may relate to persons or conduct outside the UK, which is logical given the intangible nature of electronic data. However, the powers granted under the Bill are restricted to there being some type of connection to the UK, whether because the conduct being investigated has such a link or because the data or person is within the territory.

HOW DOES IT AFFECT BUSINESS?

Internet and social media companies will be required to provide assistance under the Bill to give effect to warrants for the interception, equipment interference or retention of data. Communication service providers (**CSPs**) are at the heart of the legislation which sets out a raft of obligations with which the providers will have to comply. For example, CSPs will no longer be permitted to encrypt data so that it is unobtainable. The Home Secretary has insisted that the Bill is essential in the context of the evolving means available to criminals, terrorists and hostile foreign states to commit organised crime. There is emphasis throughout the Bill's "Guide to the Powers and Safeguards" (the "**Guide**") on the importance of the powers in tackling child sexual exploitation, serious crime cartels, organised crime and drugs running and the prevention of terrorism. This article sets out the main powers to obtain and retain communication data provided by the Bill, with additional mention of the lack of provisions in regards to confidential or indeed privileged material.

DATA COLLECTION POWERS

Interception

The definition of interception is adopted from the Regulatory Investigatory Powers Act 2000 (**RIPA**). Interception means where a person modifies, interferes or monitors a communication system, the effect of which is to make some or all of the content of the communication available in the course of its transmission to a person who is not the sender or intended recipient. Warranted interception is used for intelligence purposes and is currently covered by RIPA and the Wireless Telegraphy Act 2006. The Bill will consolidate these interception powers and limit the ability to seek interception warrants to the interception services.

COMMUNICATIONS DATA

Communications data is information about communications: the 'who', 'where', 'when', 'how' and 'with whom' of a communication but not what was said. In practice this means the fact that a person has visited Facebook, for example, will be communications data but not the content of the messages they sent while they were on there. The Guide explains that communications data will be an essential tool to "identify the location of a missing person or to establish a link (through call records) between a suspect and a victim … Sometimes communications data is the only way to identify offenders, particularly where offences are committed online, such as child exploitation or

fraud." The Bill enshrines on a revised basis the provision in DRIPA which allowed for CSPs to be required to retain certain types of communications data for up to 12 months. This has proved to be one of the most controversial aspects of the temporary legislation. The Bill inserts a number of safeguards, in an attempt to pacify those who complain that the legislation inaugurates a 'snooper's charter'.

Equipment Interference

Equipment interference comprises a wide range of activities, including remotely accessing computers to downloading covertly the contents of a mobile phone during a search. It is used by the security and intelligence agencies to interfere with equipment in order to obtain data. The Bill will consolidate the current legislation and, in addition, permit all police forces to undertake equipment interference, and introduce additional safeguards so that warrants to use these powers will require approval of the Secretary of State or Chief Constable or equivalent and the Judicial Commissioner.

Bulk Powers

Bulk interception is currently provided for under RIPA. The reference to 'bulk' powers are to the use of interception, communications data and equipment interference powers in relation to a bulk of material. The Home Secretary has stated that these powers are required in order to enable security agencies to "piece together communications and other data and identify patterns of behaviour". This power is controversial as it amounts to the ability to "trawl" large amounts of potentially irrelevant data, on the grounds that this may indicate suspicious patterns of behaviour or activity. The Bill will make explicit provision for the use of bulk powers but has limited the ability to apply for a bulk warrant to the security and intelligence agencies.

Internet Connection Records (ICRs)

An ICR is a record of the internet services a specific device has connected to, such as a website or instant messaging application. It is captured by the company providing access to the internet and is a record of the services that a person has connected to. The Home Secretary has argued that measures requiring internet service providers (**ISP**) to retain ICRs are vital for three reasons:

- to establish what services a known suspect or victim has used to communicate online which allows investigators to request more specific communications data;
- to establish whether a known suspect has been involved in online criminality, for example sharing indecent images of children, accessing terrorist material or fraud; and
- to identify services a suspect has accessed which could help in an investigation.

The Bill provides that the Secretary of State may require ISPs to retain ICR for a period up to 12 months. The Secretary of State must consider that this requirement is necessary and proportionate for the purposes of, inter *alia*, protecting the interests of national security, preventing or detecting crime or regulating financial services and markets.

OBLIGATIONS ON CSPS

The effective operation of the Bill will rely to a large extent on the co-operation of CSPs. Investigators or agencies frequently require CSPs to produce communications data relating to an individual's use of a particular service or to intercept communications sent by that service. The assistance of CSPs may also be required to gain access to

a suspect's device using equipment interference powers. The Bill consolidates the current obligations on the CSPs to provide assistance in relation to the use of investigatory powers and specifically to give effect to equipment interference warrants. Only intercepting agencies, such as GCHQ, will have the ability to serve such warrants.

LEGAL PRIVILEGE

The lack of protection in the Bill to safeguard legal privilege has been the subject of much controversy. It is proposed that a code of practice should outline the particular considerations which should be applied to data relating to a member of a profession which would "regularly hold legally privileged or relevant confidential information, such as medical professionals, those in the legal profession or MPs." In oral evidence to the Committee, the Home Secretary was challenged about the limited protection for legal privilege in the Bill. She was also asked why there is no provision in the Bill itself relating to legal privilege and why any protection should be relegated to a code of practice, which as yet is unpublished. The Home Secretary claimed that "the significance of the relationship between an individual and lawyers in discussing matters is always recognised" but that, in some circumstances, for example where a legally qualified individual was behaving improperly, it would be necessary to intercept *prima facie* privileged material. It seems that, in the Home Secretary's view, the exercise of the powers under the Bill should be available in all circumstances, when "dealing with crime and with terrorists who would seek to do us harm". There is likely to be significant debate about this issue when the Bill is put before Parliament for consideration.

CONCLUSION

Opinions divide sharply on the necessity for a bill which includes such broad and sweeping powers. However, detractors and supporters alike agree that putting those powers on an explicit and formal statutory footing will at least allow for an informed public debate to take place, and provide an opportunity for Parliament properly to challenge the extent to which the State can invade the privacy of their constituents. Only France and Sweden have put such mass surveillance powers in statute. There is an inherent tension between granting adequate powers of interception to State agencies, in order that they can effectively investigate, forestall and prosecute terrorism and cyber crimes, and the requirement to protect the right to privacy under Article 17 of the International Covenant on Civil and Political Rights, and Article 8 of the European Convention on Human Rights. It is not yet certain whether the Bill strikes the right balance between the need to protect the collective online privacy rights of the entire digital community and the imperative to protect national security and prevent serious and organised crime.

The debates in Parliament are likely to revolve around the extent of judicial oversight which the Bill provides for in granting interception and acquisition warrants, which is currently provided for by way of an Independent Commissioner and a number of specially appointed Judicial Commissioners, and whether the powers are proportionate. Parliament is likely to pay close attention to the public anxiety over the provision for the Secretary of State to require CSPs to retain browsing data for a year. Recent events such as the cyber attack on TalkTalk will be exploited by the Bill's critics to argue that it should be watered down, or torpedoed. The debates are likely to be prolonged, with a predicted coming into force date for the Bill of late this year. The proposed Codes of Practice to accompany the Bill are awaited with interest as the intention behind the legislation and guidance on

interpretation of the Bill will be critical to ensuring a robust and meaningful interrogation of its provisions. What now?

Companies should begin to assess whether they are equipped to implement the requirements of any warrant issued under the Bill, and to examine what measures they have in place to facilitate and secure data. The Committee published its report on 11 February 2016. We will issue further updates on any major developments following the publication of the report and the Government's response.

