INVESTIGATORY POWERS ACT 2016: HOW TO PREPARE FOR A DIGITAL AGE

Date: 23 January 2017

Government Enforcement Alert

By: Andrew W. Gilchrist, Christine Braamskamp, James G Millward, James G Millward

INTRODUCTION

The Investigatory Powers Act 2016 (the "**Act**") received Royal Assent on 29 November 2016. It comes into force in part in January 2017. Its main provisions include granting powers to ministers to issue warrants for intrusive surveillance; compelling internet and communications companies to retain customers' browser history for up to a year and crystallising the powers of GCHQ and MI5 to collect bulk communications data and to hack a suspect's electronic devices. It is controversial. The Act was brought in just over a month after the Investigatory Powers Tribunal criticised the security agencies for failing to process confidential data appropriately. A link to the judgment can be found here.

Its detractors have dubbed the Act the "snooper's charter" and, in scarcely more than a month since its enactment, over 200,000 people signed an on-line petition to have the Act repealed. However, it remains a core measure of the Conservative Government, with former Prime Minister David Cameron at the time heralding it as going "to the heart of the Government's duty to keep the British public safe". And, on 15 March 2016, Theresa May commended it to the Commons with the words: "The Government are committed to updating and consolidating our country's investigatory powers in a clear and comprehensive new law that will stand the test of time." In spite of the criticism from Human Rights activists, the Act is here to stay. A detailed analysis of the draft Bill was set out here. This article will focus on the main provisions of the new Act and assess what impact it may have on companies across industry sectors.

BACKGROUND

Following scrutiny of the Bill, the Intelligence and Security Committee recommended that "privacy protections should form the backbone" of the legislation. Theresa May, then Home Secretary, in response confirmed that "privacy is hardwired into the Bill". The legislation has met with significant unease among businesses, including Google, Facebook and Microsoft, who are uneasy about the prospect of diluted encryption and the requirement to store more information about customers. One of the chief reasons for their anxiety is the requirement, set out at section 87, for telecommunications operators to save the internet and communications history of everyone in the UK for a 12 month period. The Home Office has conceded that certain provisions in the Act will need to be tested and may not come into force for some time. The Act runs to 272 sections, with ten schedules and additional Codes of Practice.

WIDE AS THE OCEAN – ANY BUSINESS MAY BE CAUGHT

A business in any industry may be caught by the Act. International businesses which operate in the UK may also be subject to the Act, as many of the powers are extra-territorial. In some cases, international organisations may be required by the Act to take steps outside the UK to give effect to a UK warrant or notice. Furthermore, the Act will not only have application to the telecommunications industry. The definition of "Telecommunications operator" is buried in section 261 of the Act but, critically, includes any person who offers or provides a telecommunications service to anyone in the UK, or controls or provides a telecommunication system which is in the United Kingdom, or controlled from the United Kingdom. This definition clearly encompasses both public and private network and services providers and applies to *any* business - in whatever industry - which creates, manages or stores communications transmitted, or which may be transmitted, by a telecommunications system.

The definition of "communication" is also wide. This covers any speech, music, sound, visual image or "data of any description" as well as "signals" which are made person to person or person to machine. It is clear that most businesses will fall within the ambit of the Act. Although no obligation arises under the Act to maintain a capability to conserve or process data unless a warrant has been served, companies need to be aware of the requirements which may be made of them under a warrant. Therefore, in advance of being served with any such warrant, companies will need to put in place appropriate measures to be able to comply with the terms of the warrant.

THE ACT IN BRIEF

The Government has emphasised the importance of the Act in giving powers to the security services to "disrupt terrorist attacks" in a digital age. The key message seems to be that government must be cruel to be kind. An overview of the principal powers available under the Act is set out below:

- **Retention of communications data**: under section 87 telecommunications operators, i.e., internet and telephone providers, may be required to retain communications data for up to 12 months. "Communications data" means the metadata of individual's browsing history, i.e., the information about communications - the 'who', 'where', 'when', 'how' and 'with whom' of a communication but not what was said. Under the Act, 48 authorities, including government departments, police forces, local councils and HMRC, can request this information.
- **Equipment interference**: under this provision, the Home Secretary will be able to issue warrants to security services to hack into computers, networks, mobile devices and servers. The draft Code of Practice confirms that this includes physical interference (e.g. covertly downloading data from a device to which physical access has been gained) and remote interference (e.g. installing a piece of software on to a device over a wired and/or wireless network in order to remotely extract information from the device).
- **Bulk interception warrants**: the Home Secretary will be able to issue warrants to the security services to allow the interception of large data sets held by public and private organisations. The warrant will relate to overseas communications, i.e., those sent or received by an overseas person, and will allow extensive hacks.

- **Technical capability notices**: this is one of the most important provisions for businesses to consider. Under section 253 of the Act, the Home Secretary may require a relevant operator to maintain permanent capabilities (including the removal of encryption applied by a service provider or on its behalf, such as Whatsapp) to assist compliance with its obligations under the Act.
- **National security notice**: under section 252 of the Act, the Home Secretary may serve a notice on a telecommunications operator in order to specify measures the operator should take to facilitate, for example, the work of an intelligence agency.

WHAT NEXT?

No part of this Act is without controversy. Human rights activists are alarmed by the level of purported intrusion into individuals' private lives and companies are concerned by the potential scope of their obligations to retain, manage and de-encrypt data. Parts of the Act may be open to legal challenge. The potential for this escalated with the European Court of Justice (ECJ) ruling in December 2016 in relation to a challenge brought against the forerunner to the Act, the Data Retention and Investigatory Powers Act (DRIPA) 2014. The challenge related to the legality of intelligence agencies powers to intercept call records and on-line messages. In its finding the ECJ said: "Legislation prescribing a general and indiscriminate retention of data … exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society." The ECJ went on to state that prior authorisation by a court or independent body to access retained data must be required. As commentators have widely noted, other cases could also have implications for the Act, including an application for the judicial review of an Investigatory Powers Tribunal decision about hacking warrants and challenges in the ECJ to the EU-US Privacy Shield. The outcome of these cases may cause significant delay to the full implementation of the Act by encouraging legal challenges to its provisions.

The current Regulation of Investigatory Powers Act 2000 (RIPA), under which the *News of the World* phone hacking offences were prosecuted, will remain in force until expressly repealed. Parliament will also have to implement new secondary legislation, including the Codes of Practice that have been published in draft, but have not yet been finalised. There is therefore some way to go before the Act takes full effect.

INTERPLAY WITH DATA PROTECTION AND PRIVACY LEGISLATION

The UK is currently subject to the requirements of European data protection law, which is transposed into UK law under domestic implementing legislation. These laws, generally speaking, give individuals the right to know and control how their personal data is being processed.

While the UK remains a member of the European Union, it enjoys a pre-authorised status from the European Commission, enabling UK businesses to receive personal data in the UK from businesses located within other member states of the European Union.

If, and when, the UK leaves the European Union, this pre-authorised status will cease and the European Commission will need to assess whether the UK ensures an adequate level of protection of personal data by

reason of its domestic law or the international commitments it has entered into. It may be that the extensive powers provided to UK authorities under the Act to process individuals' personal data without their consent will cast doubt on the UK's ability to satisfy this adequacy assessment.

By way of analogy, the pre-authorised status of the US to import and process personal data from European businesses (under its "Safe Harbour" program) was recently struck down by the Court of the European Union (in October 2015). This was as a result of concerns over certain US legislation, which provided US authorities with disproportionate and indiscriminate powers to intercept, access and process personal data for the purposes of national security, public interest and law enforcement, without providing individuals with appropriate administrative or judicial means of redress.

The decision caused much disruption to US businesses which had previously signed up to the Safe Harbour program as a way of legitimising its transatlantic flows of personal data.

Any failure on behalf of the UK to qualify for such pre-authorised status would have an equally damaging effect on UK businesses. *What can businesses do?*

The Act will have almost universal application to businesses and, as part of appropriate and proportionate compliance, organisations should begin to consider whether there are any steps they could take to ensure that they have the requisite data maintenance, storage and disclosure mechanisms in place. Following the recent cases of Tesco Bank and TalkTalk, where customers' data was compromised on a severe scale, one of the overriding concerns for consumers and customers alike is whether the commercial organisations which hold their personal data – and increasingly the enforcement agencies which access the data - can manage the data securely. The reputational damage caused by being unable to comply with the requirements of an aggressive digital age may be significant.

We will continue to report on developments concerning the Act as they arise.

