Client Alert | Data, Privacy & Cyber Security / Technology

UK and EU Law Enforcement Investigatory and Data Sharing Powers: Developments and International Impact

January 2016

Authors: Detlev Gabel, Jonathan Pickworth, Robert Blamires, Tim Hickman, Jonah Anderson, Audrey Oh

Proposed UK legislation governing UK law enforcement investigatory powers (together with differences in approach by the UK and rest of Europe to law enforcement access to personal data) will have a deep and far reaching impact on technology and communications businesses, and not just those in the UK. Businesses in technology centres like the San Francisco Bay area, as well as in Taiwan, Singapore and other hubs in Asia will also be impacted. So much so in fact that US technology giants are already voicing concerns over the Bill and, rather unusually, are even attempting to intervene in the UK parliamentary process.

Introduction

On 4 November 2015, the UK government published for consultation its draft Investigatory Powers Bill[1] (the "**Bill**"), which will govern the use and oversight of investigatory powers by UK law enforcement, security and intelligence agencies, strengthen safeguards, as well as introduce new oversight arrangements.

The Bill builds on the work of three independent reviews undertaken over the past year and aims to do three things:

- Consolidate the powers already available to UK law enforcement, security and intelligence agencies to obtain the content of, and data about, communications;
- Overhaul the mechanism for authorising and overseeing these powers; and
- Ensure that the powers afforded in existing legislation are fit for the digital age.

Technology and communications businesses based not only within but also outside the UK should take note, as the Bill's extraterritorial reach could potentially require non-UK entities to assist UK law enforcement agencies, or even become subject to bulk equipment interference (*i.e.*, interception) warrants.

Impact

The Bill expands the range of organisations that will be subject to data retention and access obligations. Under previous legislation, these obligations mainly affected traditional telecoms companies. However, under the Bill, providers of so-called "over-the-top services", such as providers of messaging and other apps, are also caught (by the provisions dealing with the retention and access to communications data).

---

[1] Draft Investigatory Powers Bill, November 2015: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf.

Some notable features of the Bill are set out below:

- **Retention of Internet Connection Records** ("**ICRs**"): Communications Service Providers ("**CSPs**") will be required to keep ICRs for a maximum period of 12 months. An ICR is a record of the internet services to which devices have been connected so that law enforcement agencies can establish, for example, what services a suspect in an investigation has used to communicate online.

- **Obligations on CSPs**: CSPs can be required, under a retention notice, to retain communications data for a maximum of 12 months for access by law enforcement agencies and other public bodies. This is despite the ruling handed down last year in the *Digital Rights Ireland* case[2], in which the European Court of Justice ("**ECJ**") held that the Data Retention Directive, which required the retention of EU citizens' data for between six and 24 months, failed to comply with the principle of proportionality under the EU Charter of Fundamental Rights and constituted a disproportionate interference with both the right to a private life and the right to data protection. In addition, the Bill imposes similar obligations to comply with interception warrants and communications data acquisition notices on *all* companies providing services in the UK, or exercising control over communications systems in the UK, and also includes the requirement that CSPs provide wider assistance to law enforcement and the security and intelligence agencies.

- **Bulk powers**: The Bill makes the explicit provision for powers to access large volumes of data. In addition, the Bill will require that bulk interception and bulk equipment interference warrants may only be issued where the main purpose of the interception is to acquire intelligence relating to individuals *outside* the UK. Conduct within the UK or interference with the privacy of persons in the UK will be permitted only to the extent that it is necessary for that purpose. If this power seeks to facilitate access to overseas-related communications, private information and equipment data, the main target could be providers of cloud computing or digital/social networking-type services based overseas.

- **Encryption removal**: CSPs, when served with a notice, may be required to remove any encryption applied to assist in giving effect to interception warrants. The Bill also provides for the possibility to pass regulations imposing obligations relating to the removal of electronic protection (*i.e.*, encryption) applied by technology providers.

- **Overseas enforcement**: The Bill provides for certain obligations and powers to be enforced against overseas companies through the courts. For example, a person outside the UK may be required by notice to comply with an authorisation for obtaining communications data. The Secretary of State would enforce this duty through proceedings for an injunction or specific performance, and seeking local enforcement in the applicable overseas country using the appropriate bi- or multi-jurisdictional enforcement agreement to which the UK and the corresponding overseas country are party. For example, the UK government recognises that it will need to negotiate a mutual legal assistance treaty on intelligence with the US, which would make it legal for US companies to share data with the UK if requested under UK law.

In addition, the Bill introduces new safeguards, including:

- A "double-lock"; decisions will be taken by a Minister subject to a review by a judicial commissioner to determine whether the warrant is necessary and the conduct authorised under the warrant is proportionate. In urgent cases, a warrant can be issued without judicial approval subject to review by a judicial commissioner within five working days. There is a legitimate question however, as to whether review by a judicial commissioner either before (or in urgent cases, after) the grant of a warrant is sufficient. Perhaps a better safeguard would be for a warrant to be authorised by a judge in the first place. Recent high profile litigation generated by the grant of search warrants and surveillance warrants has exposed deficiencies in the approach taken by the state.[3]

- A new Investigatory Powers Commissioner ("**IPC**") to oversee how these powers are used (whereas the current regime is overseen by the Information Commissioner's Office, which will continue to have responsibility for enforcing data protection law). The IPC will have a significantly expanded role in authorising the use of investigatory powers and a wide-ranging and self-determined remit to oversee the use of these powers and capabilities by the security and intelligence agencies in the UK.

---

2 *Digital Rights Ireland and Seitlinger and others,* Joined Cases C-293/12 and C-594/12.

3 *R (Rawlinson and Hunter Trustees) v Central Criminal Court* [2012] EWHC 2254 (Admin), R. (*on the application of Chatwani) v National Crime Agency* [2015] EWHC 1182 (Admin), *Chatwani v National Crime Agency* [2015] UKIPTrib 15_84_88-CH.

- The Bill will also strengthen the right of redress for individuals by allowing a domestic right of appeal from the Investigatory Powers Tribunal.

The government plans to introduce a revised Bill in Parliament at the beginning of 2016, and it is expected to become law by the end of this year.

US tech firms have voiced concerns over various aspects of the Bill and are, rather unusually, attempting to intervene in the parliamentary process by submitting written evidence to the Joint Committee scrutinising the Bill. A number of tech firms have already made a submission and others are expected to do the same.[4]

Current Legislation

The law on data retention in the UK is primarily set out in the Data Retention and Investigatory Powers Act 2014 ("**DRIPA**"). The validity of section 1 of DRIPA, which provides the Secretary of State to order the retention of data for up to 12 months, is uncertain, however, after the High Court found it inconsistent with EU law in light of the *Digital Rights Ireland* case. The court has delayed the order until 31 March 2016, bringing forward DRIPA's sunset by nine months (as DRIPA is set to expire on 31 December 2016), but allowing time for debate on the Bill. In the meantime, the Secretary of State has appealed[5] the High Court's decision, and the Court of Appeal has referred questions to the ECJ.

Proposed EU Data Protection Directive for the Police and Criminal Justice Sector

The Bill is being introduced in the UK against the backdrop of the EU Data Protection Police Directive ("**Directive**"), which EU Justice Ministers agreed on 9 October 2015[6], and which forms part of the data protection reform package agreed in December 2015. The Directive aims to protect citizens' rights to data protection when their data is used by law enforcement authorities, and provides that all law enforcement processing in the EU must comply with the principles of necessity, proportionality and legality, with appropriate safeguards for the individuals.

The Directive is also intended to minimise red tape for authorities because they will no longer have to apply different sets of data protection rules according to the origin of the personal data, and further provides for general principles and clear rules for the transfer of personal data by police and criminal justice authorities outside the EU.

The agreement regarding the Directive coincides with Parliamentary scrutiny of the Bill in the UK and, conceivably, the passage of the former could impact discussions about the latter. However, the UK government has the power to opt-out of the Directive[7] and looks set to exercise that power. Consequently, businesses operating in the UK and elsewhere in Europe may find themselves subject to different compliance obligations in respect of the retention of data and law enforcement requests.

Detlev Gabel
Partner, Frankfurt
T +49 69 29994 1528
E dgabel@whitecase.com

Jonathan Pickworth
Partner, London
T +44 20 7532 1663
E jonathan.pickworth@whitecase.com

Robert Blamires
Counsel, Silicon Valley
T +1 650 213 0348
E robert.blamires@whitecase.com

Tim Hickman
Associate, London
T +44 207 532 2517
E tim.hickman@whitecase.com

Jonah Anderson
Associate, London
T +44 207 532 2293
E jonah.anderson@whitecase.com

Audrey Oh
Trainee Solicitor, London
T +44 207 532 1678
E audrey.oh@whitecase.com

4 UK Parliament Draft Investigatory Powers Bill – publications: http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-investigatory-powers-bill/publications/?type=Written.

5 *Secretary of State for the Home Department v Davis MP and others* [2015] EWCA Civ 1185.

6 European Commission Press Release, 9 October 2015 IP/15/5812: http://europa.eu/rapid/press-release_IP-15-5812_en.htm.

7 See Art.6a of the *Protocol on the Position of the United Kingdom and Ireland in respect of the area of freedom, security and justice*

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000