Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 15, NUMBER 12 >>> DECEMBER 2015

The U.K.'s Draft Investigatory Powers Bill: Intensifying the Debate over Privacy Versus National Security

By Rafi Azim-Khan and Steven Farmer, of Pillsbury Winthrop Shaw Pittman LLP, London.

U.K. Home Secretary Theresa May on November 4, 2015, unveiled the Government's proposals for what it calls "landmark legislation" in the form of the draft Investigatory Powers Bill (Draft Bill), aimed at providing law enforcement and the security and intelligence agencies with "the investigatory powers they need to keep us safe and fight crime in the digital age — subject to a world-leading oversight regime" (*see WDPR, November 2015, page 34*).

At some 300 pages long, the Draft Bill proposes a host of reforms intended to "allow security services to protect the public, and particularly children, against threats including terrorism, organised crime and sexual predators". In theory, this would be done by giving the likes of MI5, MI6 and the U.K. Government Communications Headquarters greater ability to access communications data, whilst simultaneously building safeguards around it to ensure the access is legitimate.

As analysts pore over the draft provisions, the debate has begun as to whether the proposed new powers go too far, and whether the proposed safeguards on the exercise of these powers are sufficient.

Background

The Draft Bill is designed to consolidate existing legislation on the state's ability to access communications data, *i.e.,* the "who", "when", "where" and "how" of a communication. The catalyst for this may have been the fall-out from revelations by Edward Snowden, a former employee of a contractor to the U.S. National Security Agency, about U.S. government mass surveillance practices, but the recent attacks on Paris have intensified the debate around the balance between personal privacy and national security concerns.

The Draft Bill would repeal and replace Part 1 of the U.K. Regulation of the Investigatory Powers Act 2000 (RIPA). It would also replace the emergency legislation passed in July 2014, the U.K. Data Retention and Investigatory Powers Act 2014 (DRIPA), which expires on December 31, 2016 (*see analysis by the authors at WDPR, August 2014, page 6*). DRIPA was controversially introduced in response to the European Court of Justice's judgment of April 8, 2014, in Joined Cases C-293/12

Digital Rights Ireland, which declared the EU Data Retention Directive (2006/24/EC) invalid (*see analysis at WDPR, May 2014, page 9*).

Key Provisions of the Draft Bill

The Draft Bill proposes new powers around the interception of communications, the retention and acquisition of communications data, equipment interference for obtaining (private) data, and the security and intelligence agencies' acquisition of bulk personal datasets. Needless to say, despite some concessions, the Draft Bill has attracted criticism from industry and has inherited the title "Snoopers' Charter" from the legislation it seeks to replace. The U.K. Open Rights Group, for instance, in respect of new web history retention requirements, said the move was "a step too far".

Acquisition of Communications Data

Many of the proposed powers under the Draft Bill would operate on a "warrant" or permission basis within a new oversight structure. A new, single body, led by an Investigatory Powers Commissioner, a senior judge, would replace the existing oversight arrangements split across three different bodies to establish a more visible oversight regime.

For instance, there would be powers for public authorities to acquire communications data, replacing and largely replicating the effect of Chapter 2 of Part 1 of RIPA. Requests for communications data would be made on a case by case basis, and access would be permitted only when authorised by designated senior officers within the relevant public authority on the advice of an expert "Single Point of Contact". The Draft Bill would provide for a "request filter" as an additional safeguard to prevent data from being provided to a public authority that is not directly relevant to the request, and local authority acquisition of communications data would require the approval of a magistrate.

The purposes for which communications data could be acquired other than for crime and national security would include: public health, public safety, to collect taxes, to prevent death or injury in an emergency, investigate miscarriages of justice, trying to identify someone who has died to find next of kin, and for financial regulation.

Data Retention Requirements

One of the focal points of the Draft Bill has been the proposed requirement for telecommunications operators to retain communications data for 12 months (broadly replicating Section 1 of DRIPA), and the new power for the retention of, and access to, Internet connection records. Theresa May explained that this would involve just main domains (not individual pages) along with a time/date, so that only a basic footprint could be drawn up.

Access to Internet connection records would be permitted only where it was necessary and proportionate in the course of an individual investigation, limited to three defined purposes. These would be: 1) to identify what device has sent an online communication; 2) to establish what online communications services a known individual had accessed; or 3) to identify whether a known individual had accessed illegal services online. Local authorities would not be able to acquire Internet connection records for any purpose.

The U.K. Internet Service Providers Association (ISPA), whilst accepting that law enforcement bodies should have reasonable access to data and supporting attempts at simplifying the myriad of existing laws governing the area, has raised concerns not only over the apparent "extension of existing powers" but also over a lack of clarity in terms of what is expected of ISPs, and the related costs of this activity. It would not be surprising if ISPs were forced to make major technical and infrastructural changes in the wake of new legislation, on the grounds that they may be forced to securely collect and store vastly more data than before — but this concern has not been properly addressed in the announcement.

Interception and Hacking — And the 'Double Lock'

Communications companies would be required to maintain permanent capabilities to assist agencies in exercising their powers under the Draft Bill. This would include powers to interfere with computer equipment to obtain communications, private information or equipment data.

Theresa May states that this "specific equipment interference" would serve only to bolster existing guidelines, and whilst all police forces and security agencies would be able to "hack" devices, "more sensitive and intrusive techniques" would be operated under a separate code of practice.

Warrants for the most intrusive powers — interception of communications, equipment interference by the security and intelligence agencies, and powers in bulk — would be subject to a "double-lock" authorisation process, requiring warrants issued by a Secretary of State to be approved by a Judicial Commissioner (a serving or former High Court judge) before coming into force.

However, and despite the procedural safeguards in place, there would not be (and, practically, cannot be) any prior notification or appeals process prior to interference, and some commentators have suggested that this "legitimised hacking" may erode consumer confidence in online services generally.

Bulk Data

The Draft Bill also would set out all of the agencies' powers to acquire data in bulk, including their ability to acquire communications data relating to both the U.K. and overseas in bulk from communications services providers. These powers would be subject to safeguards, including the "double-lock" process. However, concerns have been raised over the fact that such bulk collections may include data as sensitive as medical histories — at a time when even the biggest state security authorities (in the U.K. and elsewhere) are under constant bombardment from attempted cyber attacks.

   ISSN 1473-3579

Comment

Reactions to the Draft Bill have, inevitably, been mixed. For instance, whilst most accept that some access to systems is required for effective preventative policing (many welcome this being done openly with a proper framework in place), concerns still exist over authorities' ability to access data relating to individuals, such as their browsing history.

The ISPA has suggested that, more than a consolidation, the Draft Bill represents an "extension of existing powers", in particular how Internet connection records are defined. It also believes the Draft Bill's "attempts to undermine encryption could damage user trust in online services", referring presumably to obligations on communications services providers to assist the enforcement of equipment interference (*i.e.,* hacking) warrants.

From a media perspective, the U.K. News Media Association (NMA) says: "The draft Bill will not provide the level of protection across the spectrum of investigatory and other RIPA powers that has been sought previously by the media and the NMA. It contains no general right to prior notification, nor the right to contest an application before a judge, before the investigatory power is granted".

The Draft Bill will, the Government says, now go through "full pre-legislative scrutiny" before a revised Investigatory Powers Bill is laid before Parliament in the spring of 2016. For many, particularly civil liberties groups, that is insufficient time to have an informed debate over such an important — and divisive — piece of legislation, and shows a "shameful disregard" for the scrutiny required.

The text of the draft Investigatory Powers Bill is available at http://bit.ly/1l7xnjg.

The text of Home Secretary Theresa May's November 4, 2015, statement to Parliament is available at http://bit.ly/1MyNCvN.

Rafi Azim-Khan is a Partner with Pillsbury Winthrop Shaw Pittman LLP, London, and Head of Data Privacy Europe at the firm. Steven Farmer is Counsel with Pillsbury Winthrop Shaw Pittman LLP, London. They may be contacted at rafi@pillsburylaw.com and steven.farmer@pillsburylaw.com.