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 14, NUMBER 8 >>> AUGUST 2014

# The U.K.'s New Data Retention and Investigatory Powers Act 2014: Affecting Communication Services Providers Based in the U.K. and Beyond

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

The U.K. Data Retention and Investigatory Powers Act 2014 (the "DRIP Act") received Royal Assent on July 17, 2014, and came into force with immediate effect (*see report in this issue*).

This emergency legislation was passed speedily through the House of Commons and the House of Lords, being somewhat of a band aid in light of the European Court of Justice's decision of April 8, 2014, in the Digital Rights Ireland case (Joined Cases C-293/12 and C-594/12), in which it declared the EU Data Retention Directive (2006/24/EC) (the "Directive") to be invalid (*see analysis at WDPR, May 2014, page 9*).

The DRIP Act replaces the U.K. Data Retention (EC Directive) Regulations 2009 (the "Regulations"), and confirms that companies can be required to retain certain types of communications data for up to 12 months (rather than the fixed 12 months provided in the Regulations), so that this data may later be acquired by law enforcement and used in evidence.

**The DRIP Act also clarifies that anyone providing a "communication service" to customers in the U.K., *regardless* of where that service is provided from, should comply with lawful requests made under the U.K. Regulation of Investigatory Powers Act 2000.**

The DRIP Act also clarifies that anyone providing a "communication service" to customers in the U.K., *regardless* of where that service is provided from, should comply with lawful requests made under the U.K. Regulation of Investigatory Powers Act 2000 ("RIPA"). This was previously considered to be a grey area, and this clarification has significant ramifications for those providing communication services in the U.K. from overseas.

The DRIP Act is not without its critics, however. Many argue that it raises more questions than it answers and that it goes too far, especially with respect to the powers which can now be exercised against providers of communication services based outside the U.K. Subsequent legal challenges have also been lodged against it on the basis the new rules (like the old rules) continue to insufficiently protect individuals' privacy rights.

## The Data Retention Directive

The main objective of the Data Retention Directive was to harmonise EU member states' provisions concerning the retention of certain data generated or processed by providers of publicly available electronic communications services or of public communications networks.

In summary, the Directive stated that providers had to retain traffic and location data, as well as related data necessary to identify the subscriber or user, for the purpose of the prevention, investigation, detection and prosecution of serious crime. The Directive did not permit the retention of the content of communications (this being protected by privacy related legislation).

In its decision in the Digital Rights Ireland case, the ECJ found that the Directive amounted to a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, because, in a nutshell, the retention was not being limited to what was "strictly necessary". In particular, the ECJ found that the Directive was too wide-ranging in allowing data about individuals to be collected and retained even where "there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime".

When challenged by the human rights advocacy group Digital Rights Ireland (as well as privacy campaigners in Austria), the ECJ found that, by adopting the Directive, the EU legislature had not complied with the principle of proportionality, and therefore declared the Directive invalid.

## The DRIP Act

Given the Directive was invalidated by the ECJ, new rules urgently became necessary to plug potential holes in U.K. intelligence gathering capabilities that could have arisen if the companies subject to the retention requirements had stopped collecting the information in light of the ECJ's ruling.

The DRIP Act is made up of two components, which are, according to the U.K. government, "designed to strengthen and clarify, rather than extend, the current legislative framework".

The first component of the DRIP Act relates to government requirements for the retention of communications data. The second puts beyond doubt that the interception and communications data provisions in RIPA have extraterritorial effect.

### Retention of Communications Data

The DRIP Act provides power for the Secretary of State to issue a data retention notice on a telecommunications services provider, requiring it to retain certain types of communications data. It goes on to provide that the period for which data can be retained can be set at a maximum period not to exceed 12 months (rather than the fixed 12 months provided in the Regulations, which was one of the objections of the ECJ), allowing for retention for shorter periods when appropriate.

The DRIP Act goes on to provide a power to make regulations setting out further provisions on the issuance of and contents of notices, safeguards for retained data, enforcement of requirements relating to retained data and the creation of a code of practice in order to provide detailed guidelines for data retention and information about the application of safeguards.

### RIPA Provisions' Extraterritorial Reach

The second element of the DRIP Act puts beyond doubt that the interception and communications data provisions in RIPA have extraterritorial effect. Interception provides, under strict conditions and for a limited number of public authorities, access to the content of a communication.

However, the DRIP Act does not alter the existing safeguards under RIPA which regulate interception, and law enforcement and intelligence agencies will continue to need an interception warrant signed by the Secretary of State.

Specifically, Chapter 2 of Part 1 of RIPA provides a regulatory framework for the acquisition of communications data. Before a request for data can be made, necessity and proportionality tests must be carried out by a designated senior officer, at a rank stipulated by Parliament, within a public authority. Section 25(1) defines what constitutes a relevant public authority and Section 22(2) provides the purposes for which communications data may be accessed. The Secretary of State has powers to add or remove public authorities and add purposes through secondary legislation.

Regarding interception, Chapter 1 of Part 1 allows for the law enforcement and security and intelligence agencies to gain access to the content of communications made by post or telecommunications. There are a number of safeguards to ensure access is permitted only under warrant from the Secretary of State. The Secretary of State must be satisfied that the interception is necessary for the purposes of national security, the prevention or detection of organised crime, or the economic well-being of the U.K. (where this specifically relates to national security), and proportionate to what is sought to be achieved. The information must not be able to be reasonably obtained by other means.

According to the government, the DRIP Act is necessary in order to clarify the intent of RIPA. While RIPA has always had implicit extraterritorial effect, some companies based outside the U.K., including some of the largest communications providers in the market, had ques-

   ISSN 1473-3579

tioned whether the legislation applied to them. These companies often argued that they would comply with requests only where there was a clear obligation in law. The DRIP Act makes this obligation clear.

The DRIP Act also clarifies the economic well-being purpose for obtaining communications data or issuing an interception warrant under RIPA, and the definition of a "telecommunications service". This is to ensure that interception warrants can be issued and communications data can be obtained only on the grounds of economic well-being when specifically related to national security. Clarifying the definition of "telecommunications service" ensures Internet-based services, such as webmail, are included in the definition, the government says.

## Safeguards

The government says that the DRIP Act merely maintains and clarifies the existing regime and does not create any new powers, rights of access or obligations on companies beyond those that already exist. It also strengthens existing safeguards and includes a two-year sunset clause to ensure the legal framework is kept under review into the next Parliament.

In parallel, the government has announced new measures to increase transparency and oversight. These include:

- the Interception of Communications Commissioner will report every six months on the operation of the legislation;
- a senior diplomat will be appointed to lead discussions with overseas governments and communication service providers to assess and develop formal arrangements for the accessing of data for law enforcement and intelligence purposes held in different jurisdictions;
- an Independent Privacy and Civil Liberties Board will be created to consider the balance between the threat in question and civil liberties concerns in the U.K., where they are affected by policies, procedures and legislation relating to the prevention of terrorism;
- the number of public bodies currently able to request communications data will be reduced; and
- the government will publish annual transparency reports to make more information publicly available on the way surveillance powers are used.

The government has also published new draft regulations which flesh out more detail on how the new data retention powers can be exercised.

The draft Data Retention Regulations 2014 set out what information must be included in retention notices served to telecommunications companies. They also set out a number of issues that the Secretary of State issuing the notices must take into account before serving the notices.

## Comment

The passing of the DRIP Act demonstrates that the fight against crime and the protection of the public remain top priorities for the government, and such a legislative response was undoubtedly necessary in light of the ECJ's decision.

Nevertheless, the DRIP Act has attracted a fair amount of criticism, not least from civil rights campaigners Liberty, which has said it will seek a judicial review of the DRIP Act on behalf of Members of Parliament David Davis and Tom Watson.

The position of Liberty is arguably best summed up by Mr Watson: "The new Data Retention and Investigatory Powers Act does not answer the concerns of many that the blanket retention of personal data is a breach of fundamental rights to privacy", and the fact that the maximum 12 month blanket retention period for all data appears not to reflect the requirement of the ECJ's decision that retention periods should distinguish between different categories of data would certainly lend itself to Liberty's argument.

For U.S. and other foreign companies that provide U.K. citizens with services, it is also argued that the clarification that RIPA applies to them amounts to new and unprecedented powers, whilst others argue that the new definition of "telecommunication services" is too wide. In addition, importantly, the position regarding existing retention notices that communication service providers are subject to is unclear. In particular, are these automatically repealed or will they be superseded by new notices? Clearly, questions hang over the DRIP Act.

Whilst arguments rage on over the DRIP Act and questions remain unresolved, the fact is that those affected by it, including those based outside the U.K., that are providing communication services in the U.K., must be up to speed with these latest developments, whether they be categorised as clarifications of existing law or changes to it.

*The text of the Data Retention and Investigatory Powers Act, as approved by Parliament, is available at http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf.*

*The text of the draft Data Retention Regulations 2014 is available at http://www.legislation.gov.uk/ukdsi/2014/9780111118894.*

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