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.


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 is not without its critics, however. Many argue that it lacks more proportion than it merits and that it is given far too much weight that is then tensed up with respect to the privacy which can be expected against provisions of communication services based outside the U.K. Inherent legal challenges have also been lodged against it in the Supreme Court and the House of Lords, both of which have made it clear that they remain firm in their support for the protection of individuals’ privacy rights.

The Data Retention Directive

The main objective of the Data Retention Directive was to harmonize EU member states’ provisions concerning the retention of personal data generated or processed by providers of publicly available electronic communications services. It was brought into force to plug potential holes in national provisions, partly in response to ECJ’s ruling.

In summary, the Directive stated that providers had to retain traffic and location data, as well as related data, necessary to identify the subscribers or users, for the purposes of the prevention, investigation, detection and prosecution of serious crime. The Directive did not govern the retention of the content of communications (which is covered by the ECJ’s ruling). The Directive also stated that the maximum period for which data can be retained can be set at a maximum of two years, although national authorities could extend the period for shorter periods when appropriate.

The DRIP Act

The Data Retention Directive could be achieved. The information must not be able to be reasonably obtained by other means. The Secretary of State has powers to ensure access is permitted only under conditions and to a limited number of public authorities, access to the content of communications services or of public communications networks.

Regarding interception, Chapter 2 of Part 1 allows for interceptions. The interception must be 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 reasonably obtained by other means. The Secretary of State has powers to ensure access is permitted only under conditions and to a limited number of public authorities, access to the content of communications services or of public communications networks.

Retention of Communications Data

The DRIP Act provides power for the retention of serious crime, to retain data that is not limited to the retention of the content of communications. It goes on to provide that the period for which data can be retained can be set at a maximum of 12 months provided in the Regulations, which was fixed.

The DRIP Act provides power for the retention of serious crime, to retain data that is not limited to the retention of the content of communications. It goes on to provide that the period for which data can be retained can be set at a maximum of 12 months provided in the Regulations, which was fixed.

However, the DRIP Act does not alter the existing safeguards under RIPA which regulate interceptions, and the enforcement and intelligence agencies will continue to be bound by the interception warrants issued by the Secretary of State.

Retention of Communications Data

The DRIP Act provides power for the retention of serious crime, to retain data that is not limited to the retention of the content of communications. It goes on to provide that the period for which data can be retained can be set at a maximum of 12 months provided in the Regulations, which was fixed.

The DRIP Act provides power for the retention of serious crime, to retain data that is not limited to the retention of the content of communications. It goes on to provide that the period for which data can be retained can be set at a maximum of 12 months provided in the Regulations, which was fixed.
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 introduces new safeguards and includes a sunset clause to ensure the legal framework is kept under review into the next Parliament.

Safeguards

The passing of the DRIP Act demonstrates the fight against crime and the protection of the public remains a top priority 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 Davies and Tom Watson.

The position of Liberty is arguably best summed up by Mr Watson: "The new Data Retention and Investigatory Powers Act tries to 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 lead much to Liberty’s apparent consternation.

For U.K. and other foreign companies that provide U.K. telecoms services with services, it is also argued that the clarification that RIPA applies to them amounts to new and unanticipated powers, whilst others argue that the new definition of ‘telecommunication services’ is too wide.

Powers Acts, importantly, the position regarding retention periods unless that communication service provider providers are subject to in much the same way providers for those under the Data Retention and Investigatory Powers Act, already have the right to obtain interception warrants under RIPA, and the definition of ‘telecommunication services’ now covers Internet-based services, such as social networking services.

The position of Liberty is arguably best summed up by Mr Watson: "The new Data Retention and Investigatory Powers Act tries to 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 lead much to Liberty’s apparent consternation.

For U.K. and other foreign companies that provide U.K. telecoms services with services, it is also argued that the clarification that RIPA applies to them amounts to new and unanticipated powers, whilst others argue that the new definition of ‘telecommunication services’ is too wide.

Powers Acts, importantly, the position regarding retention periods unless that communication service provider providers are subject to in much the same way providers for those under the Data Retention and Investigatory Powers Act, already have the right to obtain interception warrants under RIPA, and the definition of ‘telecommunication services’ now covers Internet-based services, such as social networking services, and the government will report every six months on the operation of the legislation.

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 introduces new safeguards and includes a 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 accountability. These include:

- the interception of communications warrants can be issued and communica- tion service providers to assess and develop formal arrangements for the accessing of data for law enforcement and intelligence purposes held in different jurisdictions;
- 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 on surveillance powers and surveillance law with overseas governments and communication service providers;
- the government will publish annual transparency reports to make more information publicly available on how the new data retention powers are exercised.

The government has also published new draft regulations that will explain in greater detail how the new powers will be exercised.

The draft Data Retention Regulations 2014 set out what information must be included in retention notices, and what information must be included in interception warrants under RIPA, and the definitions of ‘telecommunication services’ now also include: Internet-based services such as social networking services, and the definition of ‘telecommunication service’ is too wide.

The position of Liberty is arguably best summed up by Mr Watson: "The new Data Retention and Investigatory Powers Act tries to 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 lead much to Liberty’s apparent consternation.

For U.K. and other foreign companies that provide U.K. telecoms services with services, it is also argued that the clarification that RIPA applies to them amounts to new and unanticipated powers, whilst others argue that the new definition of ‘telecommunication services’ is too wide.

Powers Acts, importantly, the position regarding retention periods unless that communication service provider providers are subject to in much the same way providers for those under the Data Retention and Investigatory Powers Act, already have the right to obtain interception warrants under RIPA, and the definition of ‘telecommunication services’ now covers Internet-based services, such as social networking services.