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 2 >>> FEBRUARY 2015

The U.K. Government's Draft Codes to Clarify New Legislation on Communications Data Retention and Investigatory Powers

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

The U.K. government recently consulted on a proposed update of the Acquisition and Disclosure of Communications Data Code of Practice and a draft of a new Retention of Communications Data Code of Practice.

The consultation, which ran from December 9, 2014, to January 20, 2015, has now closed.

The purpose of the consultation was to glean feedback on these two draft Codes, which set out the processes and safeguards governing the retention of communications data by communications service providers ("CSPs") under the U.K. Data Retention Investigatory Powers Act 2014 ("DRIP") and its acquisition by public authorities, including law enforcement agencies, under the U.K. Regulation of Investigatory Powers Act 2000 ("RIPA").

In light of recent high-profile criticism of DRIP, the government says that the draft Codes are intended to provide clarity and incorporate best practice on the use of the relevant powers, "ensuring the highest standards of professionalism and compliance in this important aspect of law enforcement".

The consultation has, some say inevitably, generated further criticism of the government's approach to the retention and disclosure of communications data, at a time when scepticism of the government is at an all-time high.

The consultation was open to CSPs involved in the retention and disclosure of communications data under RIPA, as well as professional bodies, interest groups and the wider public.

The consultation has, however, some say inevitably, generated further criticism of the government's approach to the retention and disclosure of communications data, at a time when scepticism of the government is at an all-time high in the wake of revelations about government surveillance by former U.S. National Security Agency contractor Edward Snowden.

Background

The government says that communications data, which it describes as "the 'who, where, when and how' of a

communication but not its content", is "crucial" for combating terrorism, fighting crime and protecting children.

Following the European Court of Justice ("ECJ") decision of April 8, 2014, in the Digital Rights Ireland case (Joined Cases C-293/12 and C-594/12) holding the EU Data Retention Directive (2006/24/EC) ("Data Retention Directive") to be invalid (*see analysis at WDPR, May 2014, page 9*), the U.K. government in July 2014 introduced emergency legislation to replace the U.K. Data Retention (EC Directive) Regulations 2009 ("2009 Regulations") (which implemented the now defunct Data Retention Directive), and DRIP came into force with immediate effect (*see analysis by the authors at WDPR, August 2014, page 6*).

DRIP and the subsequent Data Retention Regulations 2014 made under it introduced a number of changes to the U.K. communications data regime in response to the ECJ judgment.

RIPA requires the Secretary of State to prepare and publish Codes of Practice relating to the exercise and performance of the powers and duties contained in RIPA. The Secretary of State must also consider any representations made about such draft Codes.

The consultation contains proposals to update the Acquisition and Disclosure of Communications Data Code of Practice (last published in 2007) and to publish a new Retention of Communications Data Code of Practice following the passage of DRIP and the Data Retention Regulations in July 2014.

Draft of the New Retention of Communications Data Code of Practice

Under DRIP, certain types of data can be retained by CSPs pursuant to the Secretary of State issuing a data retention notice.

The types of data that can be retained remain the same as those set out in the 2009 Regulations, consisting essentially of data necessary to 1) trace and identify the source of a communication; 2) identify the destination, date, time and duration of a communication; and 3) identify users' communications equipment.

The draft Retention of Communications Data Code of Practice sets out how the U.K. government seeks to implement the requirements in DRIP and the Data Retention Regulations 2014. In particular, it covers:

- the issue, review, variation and revocation of data retention notices;
- the CSP's ability to recover its costs;
- issues of data security; and
- the disclosure and use of retained data by CSPs.

For example, it clarifies that each CSP will be required to develop a security policy document setting out its internal security organisation, governance, authorisation processes, access controls, how it allocates security responsibilities and how it ensures/oversees the deletion and destruction of data.

The government's Counter-Terrorism and Security Bill, introduced on November 26, 2014, proposes to expand the categories of data which domestic companies may be required to retain under DRIP. An additional document setting out the changes that would be made to the draft Retention of Communications Data Code of Practice, should Parliament agree to these provisions, was included in the consultation.

Draft Update of the Acquisition and Disclosure of Communications Data Code of Practice

Under RIPA, law enforcement, the intelligence agencies and some other public authorities can seek access to communications data held by CSPs if they can demonstrate that access is necessary and proportionate, and is connected to a specific investigation or operation.

The Acquisition and Disclosure of Communications Data Code of Practice was last published in 2007. The government says that it has made a number of clarifications and updates to bring the Code in line with current approaches and processes, reflecting the experience of public authorities in using the Code. It has also made a number of changes in response to the ECJ judgment and recommendations by the U.K. Interception of Communications Commissioner.

The key changes are said to:

- enhance the operational independence of the authorising officer from the specific investigation for which communications data is required;
- ensure that, where there may be concerns relating to professions that handle confidential or privileged information (*e.g.,* lawyers or journalists), law enforcement should give additional consideration to the level of intrusion;
- reflect the additional requirements on local authorities to request communications data through a magistrate;
- set out new record-keeping requirements for public authorities (in response to recommendations by the Interception of Communications Commissioner to improve transparency); and
- align the Code with best practice regarding responses to public emergency calls and judicial co-operation with overseas authorities.

The draft Codes are arguably perplexing in many areas.

There is an ongoing inquiry by the Interception of Communications Commissioner into police acquisition of the communications data of journalists, the results of

   ISSN 1473-3579

which the government says it will consider in the context of this consultation.

The government was particularly interested in views on additional safeguards, such as a requirement to flag all applications for the communications data of those in professions that handle confidential information (*e.g.,* lawyers and journalists) to the Interception of Communications Commissioner, and on whether the draft Code sufficiently protects freedom of expression.

Comment

The draft Codes are arguably perplexing in many areas. For example, the draft update of the Acquisition and Disclosure of Communications Data Code of Practice suggests that communications data is not subject to any form of professional privilege, because the fact a communication took place does not disclose what was discussed, considered or advised, when communications data can arguably be every bit as intrusive as the content of a communication.

When DRIP was introduced, whilst it received cross-party Parliamentary support, there was widespread criticism of it in many quarters, particularly given the new legislation was fast-tracked, leaving little time for it to be scrutinised properly. This led The Law Society, for example, to comment that its passage was "an affront to parliamentary sovereignty and the rule of law on the grounds that there was insufficient time for parliamentary scrutiny and debate and insufficient consideration of a considered judgment of the ECJ".

In fact, DRIP is currently being challenged in the courts by way of judicial review, with claims that the legislation is incompatible with Article 8 of the European Convention on Human Rights and with Articles 7 and 8 of the EU Charter of Fundamental Rights.

The question remains whether it is time for a fundamental review and revision of the entire legislative framework for surveillance in the U.K., rather than the tinkering of old Codes and the creation of new Codes.

In response to the consultation, David Davis MP issued a statement saying that the Home Office "has taken far too long in realising that the codes of practice regulating the acquisition of, access to and disclosure of communications data are utterly unfit for purpose", and that the new proposed Codes of Practice "fall far short of what is required".

What is needed, Mr Davis says, is judicial oversight of the process, with full judicial consideration for any request to handle any confidential or privileged information, whereas: "As they stand, the proposed changes will bring little accountability or transparency to the use of communications data".

Further, "The Government should ban either interception or collection of metadata without explicit approval by a judge for journalists and lawyers, and Prime Ministerial approval for MPs. It should also consider replacing the current ministerial approval system, which has lost all credibility, and replace it with a judicial approval system for all other interventions in electronic communications".

Similarly, in a joint response, the Press Gazette and the Society for Editors say that the draft update of the Acquisition and Disclosure of Communications Data Code of Practice provides "wholly inadequate protection for journalists' sources". The response refers to the widespread alarm in the industry over the misuse of RIPA, and essentially says that it is not enough merely to acknowledge concerns relating to professions that handle confidential or privileged information. RIPA requests for journalists' phone records should carry the same safeguards as already exist under the Police and Criminal Evidence Act, the response says, with a judge being "best placed to balance the public interest in disclosure of the information versus the over-arching public interest in respecting the confidentiality of journalists' sources".

In terms of next steps, the Home Office is now analysing the responses received on the draft Codes. It has announced that it is committed to revising the Codes as necessary before laying them before Parliament for approval.

Whilst this is significant for many, not least CSPs, given the considerable headwinds faced and the deep-rooted issues which continue to exist following the consultation, the question remains whether it is time for a fundamental review and revision of the entire legislative framework for surveillance in the U.K., rather than the tinkering of old Codes and the creation of new Codes.

Further information about the consultation, including links to the draft Retention of Communications Data Code of Practice and the draft update of the Acquisition and Disclosure of Communications Data Code of Practice, is available at https://www.gov.uk/government/consultations/communications-data-codes-of-practice-acquisition-disclosure-and-retention.

Further information about the Counter-Terrorism and Security Bill is available at https://www.gov.uk/government/collections/counter-terrorism-and-security-bill.

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