WHITE PAPER

WHAT EXACTLY DOES THE UK'S NEW DATA RETENTION LAW REQUIRE?

January, 2017

SUBSENTIO
To Notice Secretly

WHAT EXACTLY DOES THE UK'S NEW DATA RETENTION LAW REQUIRE?

In December of 2016 the United Kingdom enacted the Investigatory Powers Act of 2016. The IP Act contained a novel data retention mandate, which expanded on the nation's prior data retention law. More recently the European Court of Justice handed down a ruling that struck a major blow at the IP Act.

The following details the IP Act requirements, compares them to US law, and describes the impact of the EU court ruling. The analysis is geared to American communication service providers looking to serve the UK market.

The data retention mandate governs all "telecommunications operators"

The IP Act's section on data retention applies to a broad range of CSPs. The scope of coverage includes providers of both voice communications and/or Internet access. For example, a provider of Internet access to WiFi hotspots at hotels or restaurants would fall under the Act. So would an entity that furnishes Internet access to universities. The Act also spans both network owners and "over-the-top" competitors such as web-based providers of email and text messaging. If the CSP is a website such as a social network that offers an email or texting capability, it too is covered by the law. Both public and private networks are covered.

By contrast, the US CALEA (lawful surveillance) statute reaches a narrower regulatory terrain. It covers providers of voice and Internet access but not over-the-top players or private networks.

If a CSP is based outside the UK but serves the UK market or owns facilities in the UK, it is subject to the IP Act. For example, an American VoIP provider that terminates calls in the UK is subject to the law. It is unclear how an American CSP should respond if a UK authority requests the disclosure of records stored in the US, especially if the disclosure would contravene US privacy law.

US authorities traditionally exercised similar extra-territorial powers. However, the cross-border power was curtailed by the Second Circuit Court of Appeals last year. The Court ruled that the Stored Communications Act does not authorize the collection of foreign-stored content such as emails. Consequently, the only foreign-based communications records that US law enforcement may collect are those that reveal communications metadata (e.g. the names, dates and times of a suspect's communications).

A telecommunications operator must commence its data retention program when notified by the government

The UK's secretary of state may serve notice on any telecommunications operator that it must comply with the UK data retention mandate. The notice triggers the obligation for the CSP to start complying with the mandate. A CSP may not tip off other parties that it has received such a notice.

In the US, all CSPs subject to the Stored Communications Act must comply with the Act from the date they launch service. There is no opportunity to wait for a government compliance order and no restrictions against discussing the compliance with other parties.

303-794-6936 • info@subsentio.com • www.Subsentio.com

As a practical matter, a UK provider of nationwide service to a broad cross-section of the residential market will be more likely to receive a government notice than a small business-to-business niche player. The secretary of state must make its notice decision based on many factors: the necessity and proportionality of the regulatory burden; the technical feasibility; and the cost to the CSP. The agency must also consult the given CSP. Finally, it must gain the approval of a "judicial commissioner." The judicial commissioner position was created by the IP Act as a check against abuse by the secretary.

The telecommunications operator must retain a potentially broad range of communications data

Each retention notice will dictate the "relevant communications data" to be retained. Possibly, a CSP may be required to generate a type of data that it does not already create for business reasons. By comparison, CSPs subject to US law cannot be compelled to produce communication records they do not already keep in the normal course of business.

The UK notice will also specify the length of the retention period. The maximum length is 12 months.

In addition, the notice may impose related "requirements or restrictions." These regulatory add-ons are meant to ensure that retained data is disclosed efficiently and effectively. The open-ended nature of the provision indicates UK law enforcement might require a covered CSP to develop certain data retention technology. In the US, records need not be disclosed through any particular technology.

The IP Act term "relevant communications data" means information identifying any or all of the following, as listed in a given notice:

a. the sender or recipient of a communication;
b. the time or duration of a communication;
c. the type, method or pattern, or fact, of a communication;
d. the telecommunication system through which a communication is transmitted; and
e. the location of such telecommunication system.

The above-listed element (c) includes "Internet connection records," or "ICRs," a term that refers to website browsing histories. Under this novel rule, a CSP must log all websites visited by subscribers, as well as the dates and times of the visits. However, a website may be identified by the top level of its URL (e.g. subsentio.com), not the full IP address (which would point to a particular web site page).

The ICR portion of the mandate marks a significant expansion of data retention as practiced in the EU. Once UK law enforcement agencies are empowered to monitor a suspect's web browsing activities they can access a virtually limitless variety of intimate data about the person. Imagine all the web sites subscribers visit for personal reasons, perhaps for healthcare or financial purposes. The identities of even the most sensitive sites may now be stored and disclosed upon valid due process request by UK investigators.

Web site browsing is an exempt "information service" under CALEA. The only US mandate similar to data retention is an old rule on the books of the Federal Communications Commission that requires telephone companies to store calling records for 18 months. The US rule is far more modest than the data retention laws adopted in the E.U.

The IP Act was undercut by the EU Court of Justice

The IP Act may require significant modification in light of a December 21st ruling by the EU Court of Justice. The Court's ruling addressed a prior UK surveillance law but certainly has implications for the IP Act. Essentially, the Court said data retention mandates are permissible to fight "serious crime" but "indiscriminate" data collection violates EU privacy law. The British government has already indicated it plans to revisit the issue with the UK Court of Appeal.

UK government lawyers must now be wondering: how can we focus the IP Act on serious crime and keep it from being indiscriminate? The fact that the IP Act potentially affects all UK subscribers may itself be deemed indiscriminate. A modification may be needed to narrow that scope of coverage.

Another legal sensitivity is an issue of due process. The EU Court stated that governments should collect personal data only with the prior approval of a judge or other independent body. The IP Act does not currently contain such a requirement.

Finally, what constitutes a serious crime? The IP Act is not limited to certain crimes. In fact, it is designed for use by a wide variety of government agencies, not just law enforcement.

Assuming the British government revises the IP Act, the new version may receive more political scrutiny than the original one. The British public is known for its sophistication in matters of privacy protection. Many of them will demand the full benefit of any privacy rights recognized by the EU judiciary.

On the other hand, the EU will have no authority over the British once they revoke their EU membership. The "Brexit" may be a long and complex process but is still considered inevitable.

CSPs in the UK and elsewhere must manage a more challenging form of data retention

Based on the above, American CSPs with a presence in the UK must contend with new and controversial data retention requirements that are still in flux. Any finalized data retention mandate is bound to impose duties unfamiliar to most Americans. Therefore, US providers should analyze their networks and services in light of the changing UK law and monitor the extent of the regulatory challenge.

Budgeting to comply with a UK data retention mandate could be difficult. A CSP will not know what "relevant communications data" to retain until it receives a notice from the secretary of state. Moreover, some types of data (e.g. ICRs) may be more expensive to retain than others. Add to that the cost of information security to protect the retained data from unauthorized access. Finally, a trained staff will be needed to respond to government data requests in a manner that complies with the disclosure laws but avoids the kind of over-disclosure that may violate subscriber privacy rights.

Data retention may be necessary for public safety. But it poses significant costs and risks for the covered CSPs.

303-794-6936 • info@subsentio.com • www.Subsentio.com