

EU court strikes down security legislation over privacy concerns

by Ron Moscona

A recent decision of the Court of Justice of the European Union (“**ECJ**”) imposes restrictions on the use by member states’ law enforcement and national security agencies of telecommunication traffic and location records as tools of investigation and crime prevention.

On 21 December 2016, the court’s Grand Chamber (consisting of all its 15 judges) ruled that national legislation in the UK and Sweden imposing “general and indiscriminate” requirements on telecommunication operators to retain users’ traffic and location data was inconsistent with EU law. At issue were two cases¹ that concerned the provisions of national legislation in Sweden and the UK imposing or authorising government agencies to impose data retention requirements on service providers and requiring the disclosure of that data to law enforcement, intelligence and crime investigation agencies for investigation and national security purposes. The EU court held both the Swedish and UK legislation to be incompatible with the provisions of the Electronic Communications Directive 2002/58 (“**E-Privacy Directive**”) as read together with the provisions of Articles 7 (Respect for private and family life) and 8 (Protection of personal data) of the European Charter of Fundamental Rights (“**Charter**”). Interestingly, the challenge against the UK legislation was originally brought by a number of members of Parliament including David Davis, currently the Government minister in charge of Brexit negotiations.

The decision of the ECJ follows a previous ruling in 2014 in the *Digital Rights Ireland* case² in which the ECJ invalidated Directive 2006/24, a legislation of the European Parliament and the EU Council that imposed a data retention requirement on telecommunication providers which was similarly sweeping.

The E-Privacy Directive protects the right to privacy and confidentiality of electronic communications. Under Article 15(1) of the directive, member states may restrict the scope of certain of its provisions, by legislation, “when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and the prevention, investigation,

Related People

- Ron Moscona

Related Capabilities

- Privacy & Social Media
- Telecommunications

detection and prosecution of criminal offences or of unauthorised use of the electronic communication system". According to the ECJ's decision, it follows that member states' legislation imposing data retention obligations on service providers and access rights to that data must be subject to these requirements.

The ECJ commented that traffic and location data "allow very precise conclusions to be drawn about the private lives of the persons whose data has been retained" and allow a profile of the individuals concerned to be established. The ECJ concluded that "general and indiscriminate retention" was a "very far-reaching" and "particularly serious" interference with Articles 7 and 8 of the Charter, as data is retained without informing the individuals concerned, which is likely to cause them "to feel that their private lives are the subject of constant surveillance".

The ECJ accepted that the E-Privacy Directive and the Charter would not preclude targeted retention of traffic and location data, provided that the retention of data is limited to what is "strictly necessary", with respect to (i) the categories of data to be retained; (ii) the means of communication affected; (iii) the persons concerned; and (iv) the retention period adopted. According to the decision, targeted retention of data based on justified suspicion is permissible, however, running analysis on large databases in order to establish and justify a suspicion is not.

In relation to crime prevention, the ECJ commented that only the objective of fighting "serious crime" is capable of justifying an interference with the fundamental rights under the Charter. Further, the court pointed out that national legislation should require that adequate protections are put in place in order to protect the data, as well as ensuring that the retained data is irreversibly destroyed at the end of the data retention period.

To meet the requirements set out in the judgment, national legislation imposing data retention obligations would need to rely on specific criteria and objective evidence to justify retention obligations in specific cases in respect of particular individuals or categories of individuals whose data is likely to reveal a link, at least an indirect one, with serious criminal offences or terrorism and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. The ECJ pointed out that geographical criteria could be set for such retention requirements, where evidence shows that there exists, in one or more geographical areas, a high risk of preparation for or commission of serious criminal offences. For example, data could be retained specifically in respect of users who recently visited an area associated with terrorist activity (a topical issue in Europe, where thousands of European residents have travelled to Syria over the past couple of years to join forces with different sides in the civil war).

With regard to access to retained data, the ECJ reaffirmed that access must be limited to what is "strictly necessary" and that general access by law enforcement and security agencies to all retained data, regardless of whether there is any direct or indirect link to preventing serious crime is more than what is strictly necessary. For the objective of fighting serious crime, access can, as a general rule, be granted only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime.

The ECJ ruled that national legislation must lay down the substantive and procedural conditions governing the access to any retained data. Access to retained data should be “subject to prior review by a court or an independent administrative authority”, except in cases of “validly established urgency”. Any such authorisation should be based on objective evidence, demonstrating a likelihood that the data may establish a link with serious criminal offences, which will thereby contribute to fighting serious crime or to preventing a serious risk to public security. The ECJ also ruled that persons whose data was accessed should be notified as soon as such notification would no longer jeopardise the investigation.

The ECJ’s decision raises serious practical obstacles to governments, as it restricts their ability to utilise readily available data in connection with matters of public security and the prevention of crime and law enforcement. Legislatures will need to go back to the drawing board and draft legislation in a more guarded way in order to withstand future legal challenges.

New UK legislation, the Investigatory Powers Act 2016 (“**IPA 2016**”), which includes provisions replacing the data retention provisions that were the subject of the ECJ’s ruling, received Royal Assent on 29 November 2016, before the guidance of this judgment became available. The case will return to the UK Court of Appeal for its decision following the ECJ’s interpretation and current powers will therefore remain in place for the time being. However, in light of this recent decision, it now seems likely that the relevant provisions of the IPA 2016 may also become vulnerable to legal challenge.

¹ Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB and Watson*)

² Joined cases C-293/12 and C-594/12