TECHNOLOGY AND INNOVATION

ePrivacy: CJEU places restrictions on mass surveillance in decision on data collection and retention by electronic communications providers

October 2020

CJEU finds that national laws on the collection and retention of traffic and location data for combating crime or safeguarding national security are unlawful due to serious interferences with fundamental rights.

Colin Rooney
Partner, Technology and Innovation
+353 1 920 1194
colin.rooney@arthurcox.com

Rob Corbet
Partner, Head of Technology and Innovation
+353 1 920 1211
rob.corbet@arthurcox.com

Eoghan Clogher
Associate, Technology and Innovation
+353 1 920 1405
eoghan.clogher@arthurcox.com

The Court of Justice of the European Union (the "**CJEU**") has delivered two judgments confirming that the ePrivacy Directive applies to national legislation that requires companies to collect or retain traffic and location data for the purpose of combating crime or safeguarding national security.

The CJEU has found that EU law renders it unlawful for the electronic communications services companies ("**Elcos**") to retain and collect communications data in a general and indeterminate manner, even for the purpose of safeguarding national security.

However, a Member State facing a serious threat to national security can continue to require the general and indiscriminate retention of data relating to electronic communications for a period that is limited in time to what is strictly necessary.

In this briefing, we examine the key obligations for Elcos as a result of these rulings.

BACKGROUND

The two decisions considered by the court concerned four cases that were referred to the CJEU from national courts in the UK, France (x2) and Belgium respectively. A key issue in these cases centred on how the ePrivacy Directive impacts the way in which governments combat crime and terrorism. In particular, those cases concerned the lawfulness of national legislation which require Elcos to retain or collect users' traffic and location data in a "general or indiscriminate way".

These four cases were brought before the relevant authorities by various data privacy advocacy groups.

This is not the first time that the CJEU has ruled against laws that permitted the retention of data for law enforcement purposes. A 2014 CJEU decision in *Digital Rights Ireland and Others* (C-293/12 and C-594/12) invalidated the Data Retention Directive on the grounds that blanket data collection violated the EU Charter of Fundamental Rights, in particular the right of privacy.

The two recent decisions come just a few months after the CJEU's landmark ruling in Schrems II, where government surveillance was a key factor in the court's decision to invalidate the EU-US Privacy Shield. For further analysis on Schrems II please see our briefing here.

WHAT ARE THE KEY ELEMENTS OF THE CJEU'S JUDGMENT?

The key principle delivered by the court is the finding that the ePrivacy Directive applies to national legislation requiring Elcos to retain traffic and location data or to forward that data to national security and intelligence authorities, for the purposes of safeguarding national security and combating crime.

This principle necessitated the further finding that EU law precludes national legislation enabling a State authority to require Elcos to carry out the general and indiscriminate retention of traffic and location data or the transmission of such data to security and intelligence agencies. The principle extends to providers of access to online public communication services and hosting service providers, which cannot retain personal data relating to those services in a general and indiscriminate manner.

The court noted that the general and indiscriminate transmission and retention of such data constitutes a particularly serious interference with the fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union, where there is no link between the conduct of the persons whose data is affected and the objective pursued by the applicable legislation.

WHAT EXCEPTIONS TO THIS RULE WERE DELIVERED BY THE COURT?

The court laid down certain circumstances in which it is permissible to require Elcos to retain, generally and indiscriminately, traffic data and location data for the purposes of combating serious crime, preventing serious threats to public security and safeguarding national security. The key findings of the CJEU are summarised as follows:

1. Serious Threat to National Security

Where a Member State is facing a serious threat to national security that proves to be genuine and present or foreseeable, the ePrivacy Directive does not invalidate laws requiring Elcos to retain, generally and indiscriminately, traffic data and location data. Such data must only be retained for a period that is limited in time to what is strictly necessary, although this time period may be extended if the threat persists. In addition, the decision imposing such an order must be subject to effective review either by a court or by an independent administrative body whose decision is binding.

In the same circumstances as set out above, the ePrivacy Directive also does not preclude the automated analysis of traffic and location data.

2. Data Relating to Specific Criteria

The ePrivacy Directive does not preclude national legislation requiring the real-time collection of traffic and location data, where that collection is limited to persons in respect of whom there is a valid reason to suspect that they are involved in terrorist activities and is subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding.

It is also permissible to order the targeted retention of traffic and location data which is limited according to the categories of persons concerned or using a geographical criterion. Such targeted retention must be based on objective and non-discriminatory criteria and limited in time to what is strictly necessary. Similarly this time period may be extended if such retention continues to be necessary.

Likewise, the ePrivacy Directive does not preclude the general and indiscriminate retention of the civil identity of users of electronic communications systems, or the IP addresses assigned to the source of an internet connection. However, the IP addresses must be retained for a period limited in time to what is strictly necessary for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security.

3. Serious Criminal Offences or Attacks on National Security

The ePrivacy Directive does not preclude an instruction requiring the expedited retention of traffic and location data in the possession of Elcos where such retention is only permissible for a specified period of time and for the purposes of combating serious crime and safeguarding national security.

WHAT ARE THE NEXT STEPS?

It is likely that these rulings will have far-reaching implications for both the retention and the collection of mass communications data across Europe, and possibly for the prospects of the UK achieving a data adequacy decision once Brexit has been finalised.

Elcos must ensure that they are aware of the applicable requirements of the ePrivacy Directive and that they become familiar with the stricter rules and parameters laid down by the court for the general and indiscriminate transmission or retention of traffic data and location data. These Elcos should strive to understand the exact scope of their obligations and the circumstances in which they are permitted to accede to a request by a security or intelligence agency to carry out the general and indiscriminate transmission or retention of traffic data and location data.

The court has left room for Member States to interpret certain aspects of these rulings. For example, the rulings did not define what is meant by a 'serious threat to national security', and national legislation must provide objective and non-discriminatory criteria upon which certain decisions authorising the collection or retention of traffic and location data must be based. Therefore, the exact scope of situations warranting the permitted collection or retention of such data remains to be seen. We await further guidance on these rulings from the Data Protection Commissioner and the European Data Protection Board.

The case numbers are: C-511/18 and C-512/18 La Quadrature du Net and others; C-520/18 Ordre des Barreaux Francophones and Germanophone and Others; and C-623/17 Privacy International.

Please also see our recent analysis on Law Enforcement Requests here.

The authors would like to thank Clíodhna Golden for her contribution to this article.