

EU Court Strikes Down Security Legislation Over Privacy Concerns

January 19, 2017 – The TMCA

by Ron Moscona



In a decision published on 21 December 2016, the Court of Justice of the European Union (“ECJ”) invalidated legislation in two EU member states – the UK and Sweden – requiring telecommunication operators to retain users’ traffic and location data for 12 months and giving access to that data to intelligence, security and criminal investigation

authorities. The ECJ criticised the UK and Swedish legislation as imposing “general and indiscriminate” data retention requirements which it said were incompatible with EU law.

Similar considerations led the ECJ in 2014 to invalidate an EU directive that also required a 12 month retention period for communications data and the same concerns played a key part in the invalidation by the ECJ, in October 2015, of the Safe Harbor scheme for the transfer of personal data from the EU to the U.S. (now replaced with the new EU-US Privacy Shield).

The EU court ruled that member states’ legislation imposing data retention obligations on telecom operators must define specific conditions for a retention requirement which must be supported by objective evidence before retention obligations can be imposed in specific cases. At the same time the court acknowledged that in some cases more general retention requirements could be justified, for example, based on geographical criteria (such as the retention of communications data of users who recently visited a war zone or other area generally associated with terrorist activity).

The ECJ held that access by security agencies to the communications data must be limited to what is “strictly necessary” and that general access to all traffic and location

Related People

- Ron Moscona

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

data, even if it can be useful for preventing serious crime, is more than what is 'strictly necessary'. For the objective of fighting crime, the court held, 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 and, except in extreme urgency, must be subject to the prior oversight of the courts.

The ECJ also ruled that persons affected must be notified that their data has been retained and accessed "as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities".

The ECJ's decision raises serious practical obstacles to governments hoping to utilise readily available communications data for purposes of national security and crime prevention.

The decision coincides with the legislation coming into force in the UK which, among other things, replaces the provisions on retention of communications data and access to that data that were struck down by the ECJ. The new legislation introduces a more comprehensive scheme incorporating many new procedures and safeguards for the protection of privacy. Fresh challenges, however, may now be brought against the new legislation which will have to be assessed against the standards set out by the ECJ.