AG Opinion on compatibility of data retention with EU law

On 19 July 2016, Advocate General Henrik Saugmandsgaard Øe issued a non-binding opinion ('Opinion') that a national obligation on communications providers to retain data relating to electronic communications may be compatible with EU law, subject to certain strict safeguards. In particular, the legislation must be accessible and the obligation must respect the essence of the right to respect for private life and the right to the protection of personal data. However, it can only be lawful if it is necessary to fight serious crime, and it must be proportionate. Rohan Massey, Partner at Ropes & Gray LLP, discusses the Advocate General's Opinion and the background to the case.

Background

In its judgment in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, the Court of Justice of the European Union found that the Data Retention Directive (2006/24/EC) ('Directive') was invalid. The Court of Justice of the European Union ('CJEU') found that the Directive amounted to a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what was strictly necessary.

Since then, Member States have moved to introduce national legislation allowing for data retention. In the UK, this took the form of the Data Retention and Investigatory Powers Act 2014 ('DRIPA'), which the UK Government announced it was introducing as emergency legislation in July 2014. DRIPA replaced the Data Retention (EC Directive) Regulations 2009, under which domestic companies can be required to retain certain types of communications data (but not the actual content of a communication) for up to 12 months, so that this may later be acquired by law enforcement and used in evidence. DRIPA also clarifies that anyone providing a communications service to customers in the UK, regardless of where that service is provided from, should comply with lawful requests made under the Regulation of Investigatory Powers Act 2000.

The Conservative MP, David Davis (now the Brexit minister), and the Labour MP, Tom Watson, subsequently brought judicial review proceedings challenging the validity of DRIPA as being contrary to EU law, as expounded in *Digital Rights Ireland*. The High Court found that Section 1 of DRIPA, which empowered the Secretary of State to require telecommunications companies to retain communications data for various purposes, was unlawful.

The Secretary of State appealed the High Court decision and the Court of Appeal referred two questions to the CJEU. The questions concern whether, in *Digital Rights Ireland*, the CJEU had intended to lay down mandatory requirements of EU law with which the national legislation of Member States must comply, and whether it had intended to expand the effect of Articles 7 and/or 8 of the EU Charter of Fundamental Rights beyond the effect of Article 8 of the ECHR, as established in the jurisprudence of the European Court of Human Rights.

At present, there is also a Swedish case before the CJEU concerning the general obligation imposed in Sweden on telecommunication service providers to retain data relating to electronic communications. In that case, the Swedish telecommunications provider, Tele2 Sverige, following the decision in *Digital Rights Ireland*, notified the Swedish post and telecommunications authority that it had decided to cease retaining data and proposed deleting the data already retained. Swedish law currently requires providers of electronic communication services to retain certain personal data of their subscribers.

In both the Swedish and the UK cases, the CJEU is essentially being asked to consider whether a general obligation to retain data is compatible with EU law, in particular the e-Privacy Directive (2002/58/EC) and the EU Charter of Fundamental Rights ('Charter').

Opinion

The Opinion acknowledges that Member State laws imposing retention obligations on communications providers may be useful in fighting serious crime, such as terrorism, but that the retention of such big data poses "grave risks" to individuals' rights, which must be addressed by examining the necessity and proportionality of such obligations and balancing such risks against individuals' rights to privacy and data protection. This means that Member State laws obliging such data retention may be compatible with individuals' fundamental rights under EU law, only where there are certain strict safeguards in place. However, the Opinion clarifies that it is up to national Member State courts to determine whether such safeguards have been met.

The Advocate General notes that both UK and Swedish retention laws require communications

providers (e.g. telephony, electronic messaging and internet service providers) to retain data enabling the identification and location of the source and destination of communications, as well as the time, date, duration and type of each communication and the equipment used (but not the content of the communications themselves).

The Advocate General dismissed the notion that national data retention obligations should be excluded from the requirements of the e-Privacy Directive given that such obligations are intended to only grant access to communications data by police or judicial authorities for the purposes of public security, defence, state security and state activities in areas of criminal law. Instead, given that *inter alia* the e-Privacy Directive directly provides for the possibility of Member States adopting legislative measures for the retention of data for a limited period, such obligations must fall within the scope of the e-Privacy Directive.

However, as above, the Advocate General opined that national Member State laws can be interpreted as being consistent with the e-Privacy Directive and the Charter, provided the retention obligation:

1) has a legal basis - this means that the retention obligation must be enshrined in legislative or regulatory measures (i.e. not case law, nor non-binding codes or guidelines etc.) which are adequately accessible and foreseeable (i.e. sufficiently precise to enable individuals to regulate their conduct), and must also provide 'adequate' protection against arbitrary interference and clarify the scope and manner of exercise of the powers granted to the relevant authorities;

2) observes the essence of the rights enshrined in the Charter - this means the essence of the rights to respect for private life and to protection of personal data should not be adversely affected. The Opinion sets out that this condition is likely satisfied in the present case given that the UK and Swedish retention obligations do not extend to the actual content of communications and equivalent safeguards are implemented in respect of any personal data retained under the current EU data protection regime;

3) pursues an objective of general interest recognised by the EU - the Advocate General held that whilst the fight against international terrorism and serious crime in order to safeguard international and public peace and security would both constitute objectives of general interest to the EU, combatting 'ordinary' (as opposed to 'serious') offences and the smooth conduct of proceedings other than criminal proceeds, were not;

4) is appropriate and strictly necessary to achieve that objective - the Advocate General determined that a general retention obligation could be appropriate on the basis it would be liable to contribute to the fight against serious crime (primarily because of the utility of being able to examine the past by consulting data retracing the history of communications of certain individuals (even before they are suspected of being connected with a serious crime)). As to necessity, the Advocate General held that a measure would only be strictly necessary if no other measures existed that were at least equally appropriate but less restrictive, and provided the retention obligation imposes certain safeguards. Such safeguards, according to the Advocate General, broadly include that: (i) access and use of retained data must be limited to the recognised objective (i.e. preventing, detecting and conducting criminal prosecutions in respect of serious crime); (ii) access to retained data must require prior review from a court or independent administrative body which seeks to limit access to, and use of, the retained data to what is strictly necessary (and where, in circumstances of extreme urgency, access is granted without such a review having taken place, an *ex post facto* review must be undertaken without delay); (iii) the retained data must be held by communications providers within their relevant national territory; and (iv) retention periods must be based on objective criteria to limit retention of such data as is strictly necessary and provide for its complete destruction when no longer needed; and

5) is proportionate, within a democratic society, to the pursuit of that same objective - according to the Advocate General, this means that that the serious risks engendered by the retention obligation, in a democratic society, must not be disproportionate to the advantages which it offers in the fight against serious crime. The Opinion highlights that the retention of communications data risks interfering with individuals' rights, most of whom will never be connected in any way to serious crime, and explains that such retention may also seriously increase the risk of profiling and 'cataloguing' of the entire population of a country, which could have a detrimental effect on individuals (whether or not content data is retained) and is potentially open to abuse. However, the Opinion makes no comment as to the UK and Swedish regimes in this respect - instead (as with each of the other conditions), it leaves it up to the courts of the relevant Member

The ISPA responded to the Advocate General's Opinion by saying that it raised "serious questions about UK data retention legislation"

States to determine compliance with this condition.

Comment

DRIPA actually expires at the end of 2016, to be replaced by (the UK Government hopes) the Investigatory Powers Bill ('Bill'), the second version of which was laid before Parliament on 1 March 2016, amidst continued criticism from industry. The Bill, which has already passed through the House of Commons and is currently at Committee stage in the House of Lords, sets out the powers available to the police, security and intelligence services to gather and access communications and communications data, bulk personal datasets and other information in the digital age, subject to what the Home Office calls, 'strict safeguards and world-leading oversight arrangements.' It replaced the first version of the Bill introduced by the UK Government in November 2015, which the UK Government said responded to the concerns raised by various parties at that time. However, industry was still sceptical, with the Internet Services Providers' Association ('ISPA'), expressing disappointment that the Bill had been fast-tracked, and the News Media Association commenting that it still did not include adequate safeguards to protect journalists' sources.

The ISPA responded to the Advocate General's Opinion by saying that it raised "serious questions about UK data retention legislation." ISPA's Chair, James Blessing, said that the Opinion "calls into question some aspects of the Investigatory Powers Bill." He called on the Home Office to "ensure the legal framework around data retention is fully compliant with the final court judgement. It is vital to give industry certainty on what the rules are, maintain user confidence in online services and avoid another round of lengthy legal proceedings," he said.

As for Brexit, even if the UK does not become part of the EEA, it will not be able to ignore CJEU rulings on the lawfulness of data retention rules within the EU as these will impact on the EU's assessment of the adequacy of data protection safeguards in the UK. Failure to match the EU's adequacy requirements will likely undermine the UK's ability to trade with the Single Market and individual EU countries.

In contrast to the EU's approach to legislating retention of telecommunications data, the United States does not have any mandatory data retention laws similar to the former Data Retention Directive. Furthermore, the US Constitution does not afford the same protections as the Charter's right to respect for private life and right to protection of personal data. Thus, with the absence of any data minimisation or retention requirements, US telecommunications companies are free to retain data voluntarily.

The United States has enacted its own legislation to allow law enforcement access to telecommunications information. Notably, in 1994 the US enacted the Communications Assistance for Law Enforcement Act ('CALEA'), which requires telecommunications providers to adapt their technology to ensure the ability to comply with law enforcement surveillance requests. CALEA amends the Electronic Communications Privacy Act ('ECPA'), effectively allowing law enforcement to wiretap telephone, broadband and VoIP traffic and access stored communications. Unlike the EU laws, the ECPA permits law enforcement to access the content of the communications, but only if certain procedural safeguards are met, such as the provision of a *subpoena*, court order, or search warrant.

Further, the US intelligence community has broader powers to conduct surveillance on foreign powers and agents of foreign powers suspected of espionage or terrorism under the Foreign Intelligence Surveillance Act ('FISA'). FISA enabled US intelligence agents to obtain electronic surveillance to collect foreign intelligence from a suspected foreign power for up to one year without a court order upon issuance of an order by the US Attorney General's office showing the gaining of foreign intelligence information was the 'significant' purpose of the surveillance. The information collected without a court order can include telecommunication system metadata, which is not considered communications data under US law. Telecommunications companies have the ability to challenge FISA surveillance orders in a closed FISA court. The information collected under FISA could be used for interdiction or to develop the probable cause necessary to support an arrest warrant, but could not be used as criminal evidence.

Rohan Massey Partner
Ropes & Gray LLP, London
rohan.massey@ropesgray.com

The author would like to acknowledge the assistance of his colleagues Robert Lister and Matthew Coleman in the preparation of this article.