

Technology Law

Privacy & Information Law

Data & Information Security

Data Retention, Law Enforcement Access, and the Cloud



COVINGTON
COVINGTON & BURLING LLP

*Contributed by Mark Young and Ezra Steinhardt,
Covington & Burling LLP*

The EU Data Retention Directive (2006/24/EC) (“the directive”), which requires European telecommunications providers to retain certain communications data for up to two years, has created a significant compliance burden for providers operating across the EU. In addition to this complaint from industry, civil liberties groups continue to oppose the directive on human rights and data privacy grounds. Add to this the more general fears in Europe over foreign governments’ access to data that is under the control of cloud computing service providers, and it’s easy to see why the European Commission’s review of the directive (and of the entire data protection framework in Europe) is timely. But progress has stalled. This article explores why, and explains the related concerns over law enforcement access to data in the cloud.

Objections to the Directive

The aim of the Data Retention Directive is to harmonize obligations across the EU on telecommunications providers (such as landline, cellular and broadband providers) to retain users’ communications data,¹ and to make those data available for the purpose of the investigation, detection and prosecution of serious crime. (As with all EU Directives, each Member State must transpose it into national law.) European law enforcement agencies value the regime because it guarantees them access to vast stores of potential evidence.

This sweeping law – which in many ways cuts against Europe’s extensive data privacy regime – has been controversial since it was enacted in 2006. Some Member States have refused (or, because of opposition in their legislatures, have been unable) to transpose it, while the rest have enacted somewhat inconsistent versions.² As a result, there currently is a byzantine patchwork of differing data retention obligations in Europe, which has created a nightmarish compliance burden for telecommunications providers operating across the EU.³

Civil rights groups have strongly objected to the directive since its inception. Their main argument, which they have made repeatedly over the years – most recently in a letter to the Commission in September⁴ – is that the blanket requirement for *all* communications data to be retained, regardless of whether or not a user is under any suspicion, fails a basic test of European law. The European Convention on Human Rights requires that any interference with an individual’s right to privacy⁵ must not only be *useful* for its stated purpose (i.e., fighting crime), but also be *proportionate* and *necessary* for that purpose.⁶ Proponents of this argument suggest that alternative approaches, such as shorter mandatory data retention periods or court powers for so-called “data preservation orders”, are less invasive and equally effective.

Arguments against the directive’s retention obligations based on human rights and data privacy grounds have found favour at Member State level and are being brought in Europe’s highest

Originally published by Bloomberg Finance L.P. in the Bloomberg Law Reports. Reprinted with permission. Bloomberg Law Reports® is a registered trademark and service mark of Bloomberg Finance L.P.

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.

courts. Constitutional courts in Germany, Romania, Bulgaria, Cyprus and the Czech Republic have all annulled implementing legislation intended to give effect to the directive, and a similar action is continuing in Hungary. This has led to the Commission making formal requests to Member States to take action to ensure full compliance with the directive.⁷ Meanwhile, the Irish High Court ruled this summer that a reference should be made to the Court of Justice of the European Union (CJEU) on the directive's compatibility with human rights law, effectively inviting the Court to rule on whether the directive is "necessary".⁸ While it remains difficult to predict how the CJEU will view the issue, in part because the precise wording of the reference is not yet known, one possible indication comes from a 2007 opinion of Advocate General Kokott, when, somewhat ominously, she wrote that the directive "may have to be examined one day" as to its necessity under human rights law.⁹

The Commission's Evaluation Report and Drive for Reform

Against this backdrop, the European Commission adopted in April this year a long-awaited evaluation report on the directive and at that time announced, on the basis of what it found, that it would press forward with new proposals for reform with an impact assessment in late September or early October 2011.¹⁰

Few were surprised to learn that the Commission recommended reform: while the report concluded that the directive was a "valuable tool", it also set out a laundry list of flaws with the current regime. It documented the lack of harmonisation between Member States, highlighting the range of different requirements over how long data must be retained, who may access such data, and for what reasons. The report also revealed that Member States did not even agree on the purpose of their implementing laws; almost a third created data retention obligations for the express purpose of preventing crime as well as for investigating, detecting and prosecuting it. And the report made detailed criticisms of the new funding structures created by the directive to compensate industry for the retention burden, painting the structures as unwieldy, disharmonised, and often unfair or inaccessible for smaller service providers.

More surprising, and to the great disappointment of civil liberty campaigners and data privacy advocates, was that the report devoted hardly any attention to the fundamental question of whether the directive was "necessary". Given the central importance of this issue to the directive's future, commentators were not slow to highlight the omission. In late May, the European Data Protection Supervisor ("EDPS") Peter Hustinx joined them when he published a statement drawing attention to the oversight, saying that *"Although the Commission has clearly put much effort into collecting information from the Member States, the quantitative and qualitative information provided by the Member States is not sufficient to draw a positive conclusion on the need for data retention as it has been developed in the Directive."*¹¹

Although the Commission originally indicated that it would publish an impact assessment in the fall, it later changed that

target to December 2011. It is now December and there is no still no sign of it. In fact the Commission is continuing to consult citizens and stakeholders on future options (notably on cost recovery from telecommunications providers and on the feasibility of data preservation orders), which it says will feed into an impact assessment and a proposal that we now understand will not be published before March 2012.

What, then, is causing the Commission's delay? The EDPS did point to at least one of the causes as early as May, when he wrote that the evaluation was nearly devoid of significant statistics.¹² The sparse quantitative data that was quoted, he argued, did not demonstrate that the directive was, in fact, "necessary": the evaluation itself reported that only 9 out of the 27 Member States gave the Commission any statistics on how retained data was actually being used, and whether such use had, in reality, improved law enforcement outcomes; the remainder – a solid majority of 18 States – had provided no or only anecdotal evidence of how their law enforcement agencies used retained data, and little to no 'hard data' about the benefits of that use either. This information gap left the Commission unable to demonstrate that the directive was "necessary", which at least partly explains why the question was mostly absent from the report.

While stakeholder meetings that the Commission hosted over the summer with industry and civil society groups were apparently productive, we understand that law enforcement agencies have, for a second time, been unable to provide usage statistics to the Commission. As at the time of the initial report, this has placed the Commission in a difficult position: either steam onwards and publish the impact assessment, in which case, again, it will fail to factually demonstrate the "necessity" of the directive (and end up risking a flawed reform as well) – or delay the reform. Perhaps sensibly, the Commission has picked the latter, more cautious approach.

Confusion Over Law Enforcement Data Access Powers Abounds

Whatever the reason for the on-going delay over reform of Europe's data retention rules, the manoeuvring has come at a difficult time for industry. At the time of writing (early December 2011), a widely-leaked version of a proposed new General Data Protection Regulation is making its way through Brussels and beyond, which contains several radical new concepts.¹³ (Following months of delay, the Commission is expected to publish the final proposal in late January 2012). At the same time, the issue of "privacy in the cloud"¹⁴ and law enforcement access to data is receiving significant attention in Europe given concerns over the US Patriot Act,¹⁵ and in light of growing numbers of European businesses and public sector agencies migrating their IT functions and data to cloud-based computing services.¹⁶

An incident from late September provides a flavour of European governments' and regulators' current concerns. Dutch minister Ivo Opstelten asserted that the Dutch government would bar US cloud solution providers from government tenders because of fears that such providers are vulnerable to requests to provide

data to US law enforcement agencies under the Patriot Act – including data held in European data centres. The minister argued that compliance with such a duty in respect of EU personal data would automatically breach the data security principle of the US-EU Safe Harbor, as well as the Data Protection Directive's strictures against the export of personal data to third countries.¹⁷

There are several flaws with these concerns, which often are based on a misunderstanding of the Patriot Act and the law governing government access to data both in the United States and abroad. While the Patriot Act is often portrayed as a gateway to the exercise of arbitrary surveillance power, before obtaining data – whether located in the US or overseas – U.S. law enforcement must comply with established processes. In most cases these processes require prior judicial oversight before being served, and they are also subject to challenge by the entity receiving the request. These protections are not limited to US citizens; they extend to foreign subscribers (including businesses) located outside the US. Moreover, similar laws are on the books in some EU Member States. The UK's Regulation of Investigatory Powers Act 2000, for example, potentially allows UK law enforcement agencies to access data held outside the UK in certain circumstances, provided that at least a part of the company that holds such data operates in the UK. Mr Opstelten has now stated that the Dutch government can, after all, continue to work with US cloud providers.¹⁸

Concerns over law enforcement access to data stored in the cloud are not solely directed at US powers and agencies. For example, Belgian public prosecutors recently attempted to order the US-based Yahoo! web email service to provide access to data – an attempt that has been the subject of protracted litigation, most recently in the Belgian Supreme Court.¹⁹ The Supreme Court's decision has now been referred back to the Court of Appeal for reconsideration so a final resolution for the case is still pending.

These kinds of issues are going to crop up with increasing frequency in the coming years, as the struggle between data retention and law enforcement access regimes and data privacy and human rights laws plays out at EU and national level. Many governments and enterprises share the basic concern expressed by the Dutch about the impact of cloud services on the security and privacy of their data, and about foreign government's access to such data. The recently leaked draft of the new General Data Protection Regulation promises to spark renewed debate on this topic, as it states that EU data controllers will first be required to seek authorization from their data protection authority before they can make personal data available in response to a court judgment or decision by an administrative authority in a third country. These provisions, together with the higher monetary penalties envisioned by the Regulation, are clearly intended to serve as a counterweight to pressures exerted under foreign legal regimes, such as those in the U.S.²⁰

Amidst all of the recent confusion over progress with the review of the directive and entire EU data protection framework, one thing is clear: the reforms that will take place in 2012 and beyond will have a significant impact both on telecommunications providers'

data retention obligations and the law governing access to data in the cloud, with important repercussions for enterprise, law enforcement and human rights.

Mark Young is a senior associate in the European technology and media group in the London office of Covington & Burling. His practice focuses on intellectual property, data protection and information technology law, and encompasses legislative advocacy, regulatory compliance, and IP enforcement.

Ezra Steinhardt is a trainee in the London office of Covington & Burling who has worked with the European technology and media group on data protection, privacy and other regulatory issues.

¹⁷ "Communications data" are essentially about who contacted whom, when, and for how long (sometimes also called "metadata"). Such data are distinct from the content of a communication.

¹⁸ See Report from the Commission to the Council and European Parliament, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), Part 4, accessed on 02 Oct. 2011 at http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf.

¹⁹ Indeed, Deutsche Telekom is quoted as saying that annual running costs for its data retention obligations run at around €3.7 million a year, on top of original installation costs of €5.2 million. See "Leaked report reveals big surge in call data requests", Karlin Lillington, *Irish Times*, 14 May 2010, accessed on 04 Oct. 2011 at <http://www.irishtimes.com/newspaper/finance/2010/0514/1224270357547.html>.

²⁰ See Letter to the Commission, p.2, 26 Sept. 2011, European Digital Rights and other civil society groups, accessed on 30 Sept. 2011 at http://www.edri.org/files/dr_letter_260911.pdf.

²¹ See Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (the "European Convention on Human Rights").

²² See rulings of the European Court of Human Rights including *Foxley v. UK* (App. 33274/96), 20 June 2000, 31 EHRR 25, and *S & Marper v UK* (Apps. 30562/04 and 30566/04), 4 Dec. 2008.

²³ See, for example, Press Release, Data retention: Commission requests Germany and Romania fully transpose EU rules", 27 Oct. 2011, accessed on 9 Dec. 2011 at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1248&format=HTML&aged=0&language=EN&guiLanguage=en>.

²⁴ See *Digital Rights Ireland Ltd – v – Minister for Communication & Ors* [2010] IEHC 221], 5 May 2011.

²⁵ See Opinion of Advocate General Kokott delivered on 18 July 2007, *Productores de Música de España (Promusicae) v Telefónica de España SAU* Case C-275/06, para 82.

²⁶ *Supra* note 2.

²⁷ EDPS, *Evaluation shows that the Data Retention Directive does not meet privacy and data protection requirements*, says EDPS, 31 May 2011, accessed on 02 Oct. 2011 at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-06_Data%20Retention%20Report_EN.pdf.

²⁸ *Id.*

²⁹ See Dan Cooper, "Draft EU Data Protection Regulation Leaked", 7 Dec. 2011, accessed on 9 Dec. 2011 at <http://www.insideprivacy.com/international/european-union/draft-eu-data-protection-regulation-leaked/>.

³⁰ See, for example, speech by Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, "Privacy in the Cloud: Data Protection and Security in Cloud Computing", presented at the Round-table High Level conference on Mobilising the Cloud organised by GSMA Europe Brussels, 7 Dec. 2011, accessed on 9 Dec. 2011 at <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/859>.

³¹ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 115 Stat. 272 (2001).

³² See, for example, comments by Viviane Reding in a recent speech that, "I

am reading in the press more and more about European internet companies offering a cloud computing service which stays in Europe. Just yesterday I read about a Swedish company whose selling point is that they shelter users from the US Patriot Act and other attempts by third countries to access personal data". "The future of data protection and transatlantic cooperation", presented at the 2nd Annual European Data Protection and Privacy Conference Brussels, 6 December 2011, accessed on 9 December 2011 at <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/851&format=HTML&aged=0&language=EN&guiLanguage=en>.

¹⁷ See Zack Whittaker, "Dutch government to ban U.S. providers over Patriot Act concerns", 19 Sept. 2011, accessed on 03 Oct. at <http://www.zdnet.com/blog/btl/dutch-government-to-ban-us-providers-over-patriot-act-concerns/58342>.

¹⁸ See Loek Essers, "Dutch Minister changes Patriot Act stance", 21 Sept. 2011, accessed on 04 Oct. 2011 at <http://www.networkworld.com/news/2011/092111-dutch-minister-changes-patriot-act-251092.html>.

¹⁹ Supreme Court, Nr. P. 10. 1347. n. 18 Jan. 2011.

²⁰ See Cooper, Supra no.13.