

Data retention in Europe – under attack and under review

Mark Young and Ezra Steinhardt look at the EU's Commission's evaluation of the Data Retention Directive and pending proposal for reform.

Despite occasional rumblings about the UK coalition government reviving the Interception Modernisation Programme that was proposed by Labour (*PL&B UK* May 2010, p.9), any plans to widen the scope of storage of people's Internet data in the UK largely appear to be on hold. This is probably wise given that the European Commission has finally adopted its evaluation report on the Data Retention Directive (2006/24/EC), and announced that it will begin preparing a proposal to amend the directive.

This brief comment explains the

stakeholders, and sets out the next steps in the review process.

BACKGROUND TO THE EVALUATION OF THE DIRECTIVE

The systematic retention of communications data in the EU, whenever individuals use the telephone or the Internet, is a contentious issue that over the years has inspired robust debate among Member States, industry, and data protection advocates. The Commission's evaluation report therefore was keenly anticipated, especially given that it was several months late (published 18 April). Tension between the looming

ures transposing it, also heightened expectation levels.

The requirements, under the Directive, for communications service providers to retain communications data – essentially data about who contacted whom, when, for how long and from what location – have come under attack from several quarters. Civil liberties groups and privacy advocates argue that although such retention may be useful to fight serious crime, there has never been proof that blanket retention of all European citizens' communications data is necessary and proportionate – the relevant test under European human rights law.¹ In addition to challenges in Bulgaria, Cyprus and Hungary, national constitutional courts in Romania, Germany and the Czech Republic have annulled domestic legislation transposing the directive, and the question of its legality is expected to be referred to the European Court of Justice.² Industry meanwhile observes that inconsistent application and interpretation of the directive across the EU has created an enormous compliance burden, with companies that operate across the Union facing different, and often conflicting, rules

In addition to challenges in Bulgaria, Cyprus and Hungary, national constitutional courts in Romania, Germany and the Czech Republic have annulled domestic legislation transposing the directive.

key issues that were debated leading up to the report, highlights the Commission's findings and recommendations about revising the directive that will be of most interest to industry and other

threat of Commission infringement proceedings against Member States who have failed to properly implement the directive, and recent constitutional court rulings annulling national meas-

on which service providers are required to retain data, what categories of data must be retained, and how long for. And then there is the question of who should pay for all of this, and how it impacts the market. Given all of these issues, it is unsurprising that the Commission's evaluation attracted significant interest.

The Commission began its evaluation by seeking input from Member States, Data Protection Authorities, the private sector and others in order to better understand how the directive works in practice. It seems to have taken over a year for the Commission to receive useful feedback from the Member States and, perhaps tellingly, only ten countries responded to a subsequent request for further quantitative and qualitative information explaining why retaining communications data is necessary for law enforcement. The Commission considered the feedback alongside input from the data retention expert group,³ as well as the Article 29 Data Protection Working Party (WP29), which last summer identified serious divergences in the way that the directive had been implemented at national level.⁴

This activity formed the backdrop to the December 2010 conference in Brussels, entitled "Taking on the Data Retention Directive", at which stakeholders traded firm, often diametrically opposed views on the directive. Commissioner Malmström, a former data retention skeptic,⁵ lit the blue touch paper with her opening statement that "we have to recognise that data retention is here to stay".⁶ Malmström acknowledged that differences in the way Member States have implemented the directive "exist on several important points" and that telecommunication providers have had to bear considerable costs, suggesting that provisions of the directive perhaps need to be made more precise, including regarding state compensation for the cost of retaining data. On fundamental rights, Malmström appeared to focus on the secondary issue of access to retained data and abuse of powers, without tackling the primary question about whether the initial collection and retention of data is lawful.

Suffice to say, not everyone at the conference shared Commissioner

Malmström's views. In particular, the European Data Protection Supervisor (EDPS) Peter Hustinx stated that this was "the moment of truth" for the "notorious" directive, which he described as being "without doubt the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects".⁷ Hustinx insisted that "it is still highly doubtful whether the systematic retention of communication data on such a wide scale constitutes a strictly necessary measure", and called for the directive to be withdrawn or replaced by a more targeted and less intrusive instrument unless evidence of the directive's necessity is provided.

These and other stinging criticisms at the conference⁸ had barely been levied before national measures transposing the directive came under further attack in the courts. In addition to a challenge in Cyprus, the Czech constitutional court annulled the national transposing legislation on 22 March⁹ – a decision that was swiftly endorsed by the German Working Group on Data Retention.

FINDINGS OF THE EVALUATION REPORT

The Commission's evaluation report concludes that although data retention is "a valuable tool" for criminal justice systems and for law enforcement in the EU, the directive has had a limited impact on harmonising data retention rules across the Union, especially regarding the purposes for retaining data, how long it should be retained, and whether operators should be reimbursed for costs. Given the implications and risks for the internal market and for fundamental rights, however, the Commission stated that the EU should continue, through common rules, to ensure that high standards for the storage, retrieval and use of traffic and location data are consistently maintained. The Commission therefore intends to propose amendments to the directive, based on an impact assessment exercise focusing on the following areas:

- **Purpose of data retention.** The Commission will first assess the need for, and options for achieving, greater harmonisation regarding the purpose for retaining and accessing

data. Article 1 of the directive states that data are to be retained for the purpose of "investigating, detecting and prosecuting serious crime". But the Commission found major inconsistencies between national measures regarding the purposes for which data may be retained and accessed, and that most Member States access and use retained data for purposes going well beyond those justified in the directive: definitions of "serious crime" vary widely, and nearly a third of Member States require data to be retained in relation to all criminal offences and for crime prevention generally.

- **Categories of data covered and periods of retention.** The Commission will assess whether all of the current data categories that currently must be retained under the directive are necessary, and will consider whether retention periods should be shortened. The Commission found that there is no consistent approach to these issues across the EU: several Member States specify a single period for all categories of data – ranging from two years (Poland) to three months (Cyprus, Luxembourg, Lithuania) – while five Member States have defined different retention periods for different categories of data. The Commission therefore will consider options for harmonising retention periods across the EU, including "applying different periods for different categories of data, for different categories of serious crimes or a combination of the two". These options sound as though they could be complicated to apply in practice, which is likely to be of concern for industry given that it is craving greater harmonisation and simplification in this area.
- **Operators required to comply with data retention.** The Commission did not take this opportunity to address the definition of "publicly available electronic communications services", which may lead to continued ambiguity over whether data retention obligations apply to certain operators across the EU, including web-based service providers. The Commission instead

focused on the size of the operators that are subject to retention obligations, and pledged to examine the impact on small and medium-sized enterprises (SMEs).

- **Costs and reimbursement.** The Commission acknowledged that retention obligations represent a cost to industry, especially smaller operators, and that operators are affected and reimbursed to different degrees across the Member States. To address this, the Commission will consider ways to ensure that operators are consistently reimbursed for costs that they incur for complying with data retention requirements, paying particular attention to SMEs.
- **Access to retained data.** The report found that the way retained data is used and the amount accessed varies widely between Member States (for example, while Polish authorities made one million data access requests per year during 2008-2009, Cypriot authorities made only 100 requests). The Commission will assess the need for greater harmoni-

sation regarding which authorities are able to access data and the procedures for obtaining such access. In particular, the Commission will focus on ensuring independent supervision of requests for access, and limiting the authorities that are authorised to access data.

- **Data protection and security measures.** The report identified diverging approaches towards implementing data protection principles, particularly regarding the destruction of data once retention periods expire. It also found that national laws generally fail to make it clear what technical and organisational security measures, such as authentication and detailed access log management, operators should apply. The Commission therefore will consider options for strengthening security and data protection measures, including “introducing privacy-by-design solutions to ensure these standards are met as part of both storage and transmission”. This latter suggestion reflects input from the WP29,¹⁰ and

is sure to attract the attention of industry.

In addition to the above conclusions and action points, three other aspects of the report are worth highlighting:

- **Dismissal of data preservation/“quick freeze” as an alternative to systematic data retention.** Data preservation, or “quick freeze”, is a process whereby operators that are served with a court order must retain data relating to specific individuals suspected of criminal activity as from the date of the preservation order. The Commission acknowledged that advocates of this process consider it to be less privacy-intrusive than systematic data retention, but ultimately dismissed it on the basis that most Member States do not believe that systems of data preservation are sufficient. Member States argue that while data retention results in the availability of historical data, data preservation does not guarantee the ability to establish evidence trails prior to the preservation order, does

REFERENCES

1. See Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, and rulings of the ECHR 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 December 2008.
2. On 5 May 2010, the Irish High Court granted Digital Rights Ireland Limited the motion for a reference to the European Court of Justice.
3. The “Platform on Electronic Data Retention for the Investigation, Detection and prosecution of Serious Crime”, established under Commission Decision 2008/324/EC. Its position papers are published here, http://ec.europa.eu/home-affairs/doc_centre/police/police_intro_en.htm
4. Report 01/2010 on the second joint enforcement action: Compliance at national level of telecom providers and Internet service providers with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive’ (WP 172), 13.07.2010 (see http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf).
5. For example, when sitting in the European Parliament during debates on the directive, Malmström stated that she had “so far not been convinced by the arguments for developing extensive systems for storing data, telephone conversations, e-mails and text messages. Developing these would be a very major encroachment on privacy, with a high risk of the systems being abused in many ways. The fact is that most of us, after all, are not criminals.” Strasbourg debate, 7 September 2005, www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20050907+ITEM-002+DOC+XML+V0//EN&query=INTE RV&detail=3-044.
6. Cecilia Malmström, Member of the European Commission responsible for Home Affairs, Taking on the Data Retention Directive, European Commission conference in Brussels, 3 December 2010, <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/723>.
7. Peter Hustinx, European Data Protection Supervisor, The moment of truth for the Data Retention Directive, European Commission conference in Brussels, 3 December 2010, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf.
8. See, for example, European Digital Rights keynote lecture at the conference, “What does the European Commission owe 500 million Europeans?” European Commission conference in Brussels, 3 December 2010, www.edri.org/files/Data_Retention_Conference_031210final.pdf.
9. Judgment of the Czech Constitutional Court of 22 March on Act No. 127/2005 and Decree No 485/2005.
10. Report 01/2010 on the second joint enforcement action, supra n.4
11. EurActiv.com, “Hustinx: Data retention is the EU’s most invasive tool”, 26 April 2011, www.euractiv.com/en/infosociety/hustinx-data-retention-eus-invasive-tool-interview-504243
12. EDPS, “Evaluation shows that the Data Retention Directive does not meet privacy and data protection requirements, says EDPS”, 31 May 2011, www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-06_Data%20Retention%20Report_EN.pdf

not allow investigations where a target is unknown, and does not allow for evidence to be gathered on movements of, for example, victims of or witnesses to a crime.

- **Repercussions for Member States that have yet to transpose the directive or that have annulled national measures.** Responding to the difficulties encountered by Germany, Austria, Sweden, Romania and the Czech Republic in implementation, the Commission promised to work constructively with each country to address their concerns – but, perhaps oddly (given that it now seems committed to amending the directive), the Commission also stated that it would reserve its right to commence enforcement proceedings, if necessary.
- **Implications for fundamental rights.** Having stated that Member States “generally reported data retention to be at least valuable, and in some cases indispensable,” the report later summarised European jurisprudence on limits to the right

to private life and the protection of personal data, and acknowledged the substantial criticism from civil society groups and regulatory authorities regarding data retention. The Commission did not pass further comment on this, but committed to consider the issues raised by national case law and to ensure that any future data retention proposal respects the principle of proportionality and does not go beyond what is necessary to combat serious crime.

REACTIONS TO THE EVALUATION REPORT AND NEXT STEPS

Civil liberties groups lambasted the report for failing to provide convincing evidence of the need for data retention. The EDPS was only a little more positive. He acknowledged that the report presented a “more balanced” picture of the Directive’s problems than previous drafts and welcomed that problems with the Directive were now “at least on the table”, but stated that his view of the Directive was “negative and [after the report’s publication] it still is”.¹¹ Overall, the EDPS has concluded that

the Directive does not meet the requirements imposed by the fundamental rights to privacy and data protection, and has called on the Commission to consider all options, including the possibility of repealing the Directive as well as alternative, more targeted retention measures.¹²

The next step for the Commission will be to publish an impact assessment of the specific proposals. This assessment, expected in September or October this year, is currently being shaped by a new round of stakeholder meetings and conferences taking place this summer. Ultimately the impact assessment is expected to form the basis of a new, formal proposal for the directive’s reform, which the Commission is expecting to publish as soon as the first quarter of 2012.

AUTHORS

Mark Young, is an Associate in the European Data Privacy Practice, Covington & Burling LLP and Ezra Steinhardt, is a Trainee at Covington & Burling LLP.
Email: myoung@cov.com