CENTRE FOR LAW AND DEMOCRACY

European Union

Analysis of the Data Retention Directive

July 2013

Centre for Law and Democracy
info@law-democracy.org
+1 902 431-3688
www.law-democracy.org

Introduction

In 2006, the European Parliament passed Directive 2006/24/EC (the Data Retention Directive), in part in response to the security crisis provoked by terrorist attacks in Madrid in 2004 and in London in 2005. The Directive introduced blanket telecommunications surveillance measures with important implications for the right to freedom of expression. Specifically, European Union Member States are obliged to transpose the Directive into national law, including through provisions which compel "providers of publicly available electronic communications services or of a public communications network" (service providers) to retain the traffic and location data of all users' telephone and Internet communications for between six months and two years.

The Directive has come in for widespread criticism from human rights organisations, telecom associations, IT security firms, journalists, healthcare professionals and legal experts on the basis that it violates the right to privacy and that it is costly, cumbersome and unnecessary. According to a report by the European Commission, only 9 of 27 Member States had explicitly endorsed the Directive as a necessary security measure some five years after it was first adopted.[1] Meanwhile, courts in Austria, Bulgaria, Cyprus, the Czech Republic, Germany, Ireland and Romania have rejected the Directive as unconstitutional and/or referred the matter to European Court of Justice on the basis that it violates fundamental rights. At the same time, the European Commission has taken measures against countries which have failed to transpose the directive and, on 30 May 2013, Sweden was fined 3 million Euros for failing to implement the Directive until 2012.[2]

Pursuant to Article 1 of the Directive, service providers must be required to retain the traffic and location data of all registered users. Article 5 delineates the specific categories of data to be retained, including data necessary to identify the source and destination of a communication, as well as the type, date, time and duration of the communication and the location of the communication equipment, in every case linked to information identifying the user. No data revealing the content of electronic communication may be retained under the Directive. However, the breadth of the data retained is enormous, especially when one takes into account powerful modern data mining techniques. Even fragmentary, seemingly innocuous pieces of telecommunications traffic data can be linked, matched and mined with

[1] Report from the Commission to the Council and the European Parliament, *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, 18 April 2011, COM(2011) 225 final. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF.
[2] See: http://www.huntonprivacyblog.com/2013/06/articles/sweden-fined-for-delaying-implementation-of-the-data-retention-directive/.

information from other sources, transforming them into a detailed whole and creating a detailed digital picture of an individual's life.[3]

Pursuant to the EU Charter on Fundamental Rights, any law that limits the exercise of fundamental rights and freedoms must be "necessary and genuinely meet objectives of general interest."[4] The European Court of Justice has consistently held that the test of necessity is not satisfied by mere usefulness. Specifically, "limitations in relation to the protection of personal data must apply only in so far as is 'strictly necessary'".[5] Similar standards for restrictions on both privacy and freedom of expression apply under the *International Covenant on Civil and Political Rights* (ICCPR)[6] and the *European Convention on Human Rights* (ECHR).[7]

This Analysis considers the Directive from the perspective of international and European guarantees of the right to freedom of expression. It describes the ways in which the Directive restricts freedom of expression, outlines the relevant standards which apply to restrictions on this right, and discusses the various ways in which the Directive and the way it has been transposed into national law violate the right. Finally, the Analysis contains recommendations as to measures which deliver on the objectives of the Directive while avoiding its pitfalls.

1. An Interference with Freedom of Expression

International guarantees of freedom of expression protect the right to seek, receive and impart information and ideas, or more generally the free flow of information and ideas in society. It is obvious that electronic communications are a core form of expressive conduct. In an increasingly interconnected and on-the-go world, more and more of our communication takes place electronically, via computers, mobile phones and other devices, carried over the Internet, mobile networks or traditional landlines, using voice, e-mail and social media.

[3] Helen Nissenbaum, *The Meaning of Anonymity in an Information Age* (Online Ethics Center for Engineering, 16 February 2006). Available at: http://www.onlineethics.org/Topics/EmergingTech/TechEssays/nissanon.aspx.
[4] *Charter of Fundamental Rights of the European Union*, Article 52(1). Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:0391:0407:en:PDF.
[5] European Court of Justice (ECJ), 9 November 2010, C-92/09 and C-93/09, Volker und Markus Schecke, § 86. Available at: http://curia.europa.eu/juris/document/document.jsf?docid=79001&doclang=EN&mode=&part=1.
[6] UN General Assembly Resolution 2200A (XXI), 16 December 1966, entered into force 23 March 1976.
[7] Adopted 4 November 1950, E.T.S. No. 5, entered into force 3 September 1953.

It is also beyond doubt that measures which exert an indirect chilling effect on free speech represent interferences with the right. The most explicit statement of this is found in Article 13(3) of the *American Convention on Human Rights*,[8] which states:

> The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.

But this is also implicit in cases decided under other treaties which require States to put in place fair systems for accreditation of journalists,[9] to ensure the right of journalists to protect their confidential sources of information,[10] to protect media outlets and journalists against attacks,[11] to promote pluralism in the media,[12] and to ensure that sanctions for breach of rules restricting freedom of expression are not, of themselves, so large as to exert a chilling effect on free speech.[13]

An important aspect of freedom of expression is control over the use to which one's communications are put, including who may access them. Studies have shown that the greater the perceived control an individual has over their information, the more extensive and frank their interactions will be.[14] Alternatively, the less control one has over one's communications, the higher the risk that they will be used without one's consent, and the less free one feels to express oneself.

This is a general phenomenon, which is seriously undermined by the blanket and indiscriminate data retention rules required by the Directive, which basically installs a sense in everyone that their communications may be monitored, even if they have not been involved in any criminal activity. This is exacerbated by the sense that the automatic retention of data is somehow a presumption of (at least potential) guilt, which creates the subjective perception that one is being watched in case one makes a wrong move, thereby inhibiting free, full and candid expression.

---

[8] Adopted 22 November 1969, O.A.S. Treaty Series No. 36, entered into force 18 July 1978.
[9] *Gauthier v. Canada*, 5 May 1999, Communication No. 633/1995 (UN Human Rights Committee).
[10] *Goodwin v. the United Kingdom*, 27 March 1996, Application no. 17488/90 (European Court of Human Rights).
[11] *Özgür Gündem v. Turkey*, 16 March 2000, Application no. 23144/93 (European Court of Human Rights).
[12] *Centro Europa 7 S.R.L. and Di Stefano v. Italy*, 7 June 2012, Application no. 38433/09 (European Court of Human Rights).
[13] *Tolstoy Miloslavsky v. United Kingdom*, 13 July 1995, Application no. 18139/91 (European Court of Human Rights).
[14] Tamara Dinev, Heng Xu, Jeff H. Smith and Paul Hart, "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts" 22 *European Journal of Information Systems* (2013), p. 300. Available at: http://www.palgrave-journals.com/ejis/journal/v22/n3/pdf/ejis201223a.pdf.

There are a number of specific contexts in which the perception of loss of control over communications is likely to have a particularly significant impact. These include situations where sensitive information is involved, such as contact with physicians, lawyers and psychologists, using helplines and relations between journalists and their confidential sources. Similarly, the retention of location data has a particular impact on the ability to communicate from sensitive locations such as clinics, support groups, and private dwellings or offices affiliated with political parties.

The importance of protecting communications against undue surveillance has been recognised by the UN Special Rapporteur on Freedom of Opinion and Expression:

> States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy…. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.[15]

The Directive also interferes with individuals' ability to communicate anonymously, which it has been argued is a right in a democratic society.[16] As with control more generally, anonymity is of heightened important in a number of contexts. It allows citizens to voice controversial opinions and ideas from behind the cloak of anonymity, contributing to the marketplace of ideas, inasmuch as it enables individuals to contribute perspectives which would otherwise be silenced for fear of public ridicule or censure. Without anonymity, challenging ideas may fall prey to social conformity, robbing present and future generations from divergent and dissenting but potentially beneficial ideas. Anonymity also supports socially valuable institutions such as voting, whistleblowing and peer review, and facilitates reaching out for help concerning stigmatised problems such as sexual identity, alcohol abuse, domestic violence and suicidal tendencies. A particularly valuable feature of the Internet – namely that it has substantially enhanced the ability to communicate and explore information anonymously – is thus threatened by the Directive.

These benefits are not just theoretical. For example, websites have found that anonymous users contribute the most insightful comments. In 2011, TechCrunch, a leading technology web publication, switched from allowing users to comment anonymously to requiring them instead to log into Facebook and use their real names. By January 2013, the publication had lost so many users and their valuable comments that it dropped this requirement, and asked people to come back and

[15] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, UN Doc. A/HRC/23/40, para. 79.
[16] Note, "The constitutional right to anonymity: Free speech, disclosure and the devil" 70(7) *Yale Law Journal* (1961), pp. 1084–1128.

make comments anonymously again.[17] Studies have also shown that individuals seeking health information are concerned about divulging their identity for fear that employers or insurance companies might discover what web pages they have visited.[18]

In brief, the Directive undermines individuals' confidence in their ability to control their communications, in turn exerting a chilling effect on free and frank communicative activity and undermining the free flow of information and ideas in society, i.e. freedom of expression.

2. Standard of Necessity

The test under international law for assessing whether restrictions on freedom of expression are legitimate involves three sub-tests, namely whether the restriction is provided by law, serves to protect one of the legitimate interests listed in international guarantees and is necessary to protect that interest. For purposes of this analysis, we assume that national rules meet the provided by law standard, although this may be in question in some cases, and that they serve to protect public order and/or national security, two of the legitimate interests recognised under international law. Our analysis thus focuses on the third part of the test, the requirement that restrictions be necessary to protect the interest. It may be noted that this is the part of the test upon which the legitimacy of a restriction hangs in the vast majority of international cases.

Necessity presents a high standard to be overcome by the State seeking to justify the restriction, apparent from the following quotation, cited repeatedly by the European Court of Human Rights:

> Freedom of expression, as enshrined in Article 10, is subject to a number of exceptions which, however, must be narrowly interpreted and the necessity for any restrictions must be convincingly established.[19]

"Necessary" is a complicated notion but it has been interpreted to include a number of different elements. First, international courts often assess whether or not there is a "pressing" or "substantial need" for the restriction.[20] This rules out restrictions which, although they serve to protect a recognised type of interest, do not meet a

[17] TechCrunch, Commenters, We Want You Back, 22 January 2013. Available at: http://techcrunch.com/2013/01/22/we-want-you-back/.
[18] Lee Rainie and Susannah Fox, *The Online Health Care Revolution*, Pew Internet, 26 November 2000. Available at: http://www.pewinternet.org/Reports/2000/The-Online-Health-Care-Revolution/Section-2/The-absolute-value-of-anonymity.aspx.
[19] See, for example, *Thorgeirson v. Iceland*, 25 June 1992, Application no. 13778/88, para. 63.
[20] See, for example, *Lingens v. Austria*, 8 July 1986, Application no. 9815/82, para. 39 (European Court of Human Rights).

minimum threshold test in terms of the significance or importance of the specific interest involved.

Second, the restriction must be rationally connected to the objective of protecting the interest, in the sense that it is carefully designed and represents the least intrusive measure which would effectively protect that interest. This is somehow obvious since when restricting rights one may not "use a sledge-hammer to crack a nut". As the Inter-American Court of Human Rights has held: "[I]f there are various options to [protect the legitimate interest], that which least restricts the right protected must be selected.[21] Similarly, the Supreme Court of Canada has held:

> First, the measures adopted must be carefully designed to achieve the objective in question. They must not be arbitrary, unfair, or based on irrational considerations. In short, they must be rationally connected to the objective.[22]

A closely related but different notion is that a restriction should not be overbroad in the sense that it limits legitimate speech as well as harmful speech. Once again, this makes obvious sense, since targeting legitimate speech cannot be deemed to be necessary. As the Inter-American Court has noted: "Implicit in this standard, furthermore, is the notion that the restriction, even if justified by compelling governmental interests, must be so framed as not to limit the right protected by Article 13 more than is necessary."[23] The US Supreme Court has similarly warned against the dangers of overbroad restrictions on speech:

> Even though the Government's purpose be legitimate and substantial, that purpose cannot be pursued by means that stifle fundamental personal liberties when the end can be more narrowly achieved.[24]

Finally, restrictions must meet a proportionality test, whereby the benefit in terms of protecting the interest must be greater than the harm caused to freedom of expression. Otherwise, on balance, the restriction cannot be justified as being in the overall public interest. This goes to the substance of a restriction, as well as to any sanctions imposed for breach of it.[25]

3. Why the Directive Generally Fails the Necessity Test

[21] *Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism*, Advisory Opinion OC-5/85 of 13 November 1985, Series A, No. 5, para. 46.
[22] *R. v. Oakes*, [1986] 1 SCR 103, pp.138-139.
[23] Compulsory Membership, note 21, para. 46.
[24] *Shelton v. Tucker*, 364 US 479 (1960), p. 488. See also *R. v. Oakes*, note 22, pp. 138-9: "Second, the means, even if rationally connected to the objective in this first sense, should impair "as little as possible" the right or freedom in question".
[25] See, for example, *Tolstoy Miloslavsky v. United Kingdom*, note 13.

The Directive is an extremely broad, untargeted measure which, as a result, faces a heavy presumption of invalidity as a restriction on freedom of expression. Assuming that there is a pressing social need for the measures, in the sense of a need to enhance law enforcement, the next question is whether the measure is carefully designed to achieve that objective. Nothing about the system is carefully designed. It calls for the retention of all data, just in case some of it might be useful in pursuing crime. The only protections – namely that the focus is supposed to be on "serious crimes" (mentioned only once, in Article 1) and that the data is supposed to be available "only to the competent national authorities in specific cases" (Article 4) – provide scant protection against abuse in practice (see below). As the UN Special Rapporteur on Freedom of Expression and Opinion has stated:

> States should not retain or require the retention of particular information purely for surveillance purposes.[26]

It is relatively easy to think of ways to render the rules more targeted. At a minimum, the system could incorporate far more robust protections, including clearer and clearly binding rules in relation to the two protections mentioned above.

An even more targeted alternative is data preservation. Rather than retaining data on every communication made by every citizen, data preservation entails the rapid forward looking "quick freeze" (i.e. retention) of data relating to targeted suspects, which may be released to law enforcement authorities once judicial authorisation has been obtained. "Quick freeze plus" goes further by also freezing all of the communications data which is held by service providers, for example for billing or transmission purposes.

While data preservation provides less information than a data retention regime, its targeted and procedurally safeguarded nature makes it far less problematical from a freedom of expression and privacy perspective.[27] It is worth noting that Member States that have found data retention to be unconstitutional, including the Czech Republic, Germany and Romania, are successfully prosecuting crime by means of data preservation. Moreover, the Council of Europe Cybercrime Convention refers only to data preservation as an investigative tool to combat cybercrime, and not data retention.[28]

---

[26] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, note 15, para. 90.

[27] Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 23 September 2011, para. 56. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:279:0001:0010:EN:PDF.

[28] Convention on Cybercrime, Article 16. Available at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

There is also evidence that data retention measures have only impacted in nominal ways on law enforcement. Independent studies in Germany and the Netherlands have found that requested traffic data retained under the Directive could "nearly always" be met in the absence of blanket data retention, and that only 0.01% of criminal investigations in Germany were potentially affected by a lack of communications data.[29] This suggests that the measures fail to meet the proportionality requirement of the test for necessity.

Another problem with justifying data retention is the existence of circumvention techniques, which are disproportionately likely to be used by the very individuals that the Directive targets. These include tools such as prepaid SIM cards, Virtual Private Networks (VPN) and smaller service providers not covered by the Directive. There is some evidence that even individuals who are unlikely to be the subject of investigations are drawn to these circumvention techniques, providing strong support for the argument above to the effect that people feel that their control over their communications is threatened by the measures required by the Directive. A German poll commissioned after the Directive was adopted found that nearly 60% of Germans used or intended to use service providers that did not indiscriminately retain communications data, and over 46% declared their intention to use Internet anonymisation technology.[30]

4. Specific Problems

4.1 Access to Data

The stated purpose of the Directive is to assist in the investigation, detection and prosecution of serious crime (Article 1) and only competent national authorities are supposed to be able to access retained data (Article 4). Neither of these rules is observed in practice across European Union Member States.

Article 4 fails to establish any standard rules or conditions regarding what would constitute a competent national authority or when such authorities should be able to access retained data. Instead, this is left to the discretion of Member States, in part because the European Union does not have the jurisdictional competence to legislate on law enforcement matters. This has, however, created a legal loophole that has been used to allow access to retained data for purposes other than those covered by the Directive, such as preventing and combating crime broadly speaking rather than just serious crime.

[29] European Digital Rights, *Shadow evaluation report on the Data Retention Directive (2006/24/EC)*, 17 April 2011, p. 13. Available at: http://www.edri.org/files/shadow_drd_report_110417.pdf.
[30] Infas Institute Poll, 25 January 2010. Available at: http://www.vorratsdatenspeicherung.de/images/infas-umfrage.pdf.

Member States have also granted access to retained data to a long list of "competent national authorities", including prosecutors, national police forces, military, intelligence agencies and public authorities. More worrisome, however, are cases of private individuals and businesses obtaining access to confidential data retained under the Directive. For example, the Swedish Supreme Court ruled in 2012 that copyright holders could legitimately request information on alleged copyright infringers from service providers. Preliminary questions were referred to the European Court of Justice, which found that European Law did not preclude Member States from permitting service providers to hand over confidential data collected under the Directive in cases of intellectual property infringement.[31]

There are also no standard or minimum procedural requirements for accessing retained data. Several Member States require judicial authorisation for every request, but others only require it in some cases. Several States only require authorisation from a senior (administrative) authority, while in two States – Malta and Ireland – the only standard appears to be that the request be made in writing.[32]

The UN Special Rapporteur on Freedom of Opinion and Expression has made it clear that surveillance must take place under judicial supervision:

> Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority.[33]

The gradual widening of the use of the Directive for purposes beyond that for which it was originally intended, accessed by an ever growing number of "competent national authorities" with limited or no independent oversight, seriously exacerbates the freedom of expression problems noted above. While we recognise that the European Union does not have the jurisdiction to address these problems directly, this still cannot justify the putting in place of a rule that breaches human rights. The European Union should either find an effective work around for these serious problems with the way the Directive is implemented, or do away with the Directive.

4.2 Data Security

Article 7 of the Directive requires Member States to ensure that service providers respect minimum data security principles, including measures to protect the data

[31] ECJ, Case C-461/10. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=121743&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=793630.
[32] Evaluation Report, note 1, p. 9.
[33] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, note 15, para. 81.

against unauthorised or unlawful storage, processing, access or disclosure. It would appear that many Member States, however, have failed to implement minimum data security standards, in breach of Article 7.[34] Furthermore, even the standards mandated by the Directive have been criticised by the German Constitutional Court as being insufficient and in violation of fundamental human rights.[35] Key to their reasoning is that service providers are not required to guarantee data security in a manner that can be enforced.

More generally, it is widely acknowledged that that the only truly safe data is erased data and that the most vulnerable databases are those that host the most sensitive information. As the amount of retained data increases, the threat to individuals and society grows. Data misuse occurs on a daily basis, although it rarely comes to light. For example, Citizenship and Immigration Canada suffered more than three security breaches a week in 2012, yet only five breaches were disclosed to the Privacy Commissioner of Canada that year. Virtually no Canadian department has been impervious to security breaches.[36] In many cases, breaches come to public attention only years later through insider whistleblowing.

In 2006, traffic data from 17 million users was stolen from German telecommunications giant Deutsche Telekom. In turn, Deutsche Telekom illegally used traffic data – from its own data pool as well as domestic and foreign service providers – to spy on 60 individuals suspected of being involved in the theft, including critical and investigative journalists. This large-scale abuse of sensitive data was later revealed by a single whistleblower.[37] In 2010, it was discovered that Polish police and intelligence agencies had requested and obtained traffic data of at least 10 influential journalists in order to identify their confidential sources. The data was obtained extrajudicially and outside of the scope of any criminal investigation. Despite these cases and others, the Commission continues to deny that data retention has resulted in any concrete cases of abuse.[38]

4.3 Period of Retention

Pursuant to Article 6 of the Directive, Member States must required service providers to retain data for between six months and two years from the date of the communication. Pursuant to Article 12, a Member State may extend this period for a

[34] Shadow Report, note 29, p. 8.
[35] Federal Constitutional Court of Germany (BVerfG), press release of 2 March 2010. Available at: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10- 011en.html.
[36] Michael Geist, "Your Information is Not Secure: Thousands of government breaches point to need for reform", *The Ottawa Citizen*, 30 April 2013. Available at: http://www.ottawacitizen.com/technology/Your+information+secure/8313129/story.html.
[37] German Working Group on Data Retention, *There is no secure data*. Available at: http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten_en.pdf.
[38] Evaluation Report, note 1, p. 30.

limited time should particular circumstances warrant such an extension. However, there is no provision for shortening the retention period below six months. Based on quantitative evidence provided by nine Member States in 2008, 67 percent of the data requested that year was less than three months old and almost ninety percent of the requested data was less than six months old.[39] This suggests that a maximum period of two years goes beyond what is necessary to achieve or largely achieve the purposes of the Directive. Further evidence of this is the fact that only a handful of States have opted for retention periods of longer than one year.

The negative impact of data retention on the rights to freedom of expression and privacy increases with the length of the period of retention and, in general terms, the longer the retention period, the greater the violation. The German Constitutional Court has ruled that a six-month period of data retention is near the legal limit of how much personal data governments may collect.[40] Longer retention periods also increase the quantity of data being maintained, thereby increasing the severity (or impact) of data breaches.

Recommendations:

- The Data Retention Directive should be repealed and replaced by a more carefully designed and targeted regime, along the lines of data preservation, which takes into account the extent to which the system represents an interference with freedom of expression.
- At a minimum, if the system is retained, the following measures should be put in place:
  - Safeguards against abuse of the system – in the form of limiting both the scope of activity which would justify access to data (i.e. serious crimes) and the scope of actors who can access the data – should be substantially enhanced.
  - States should be required to put in place strong data security measures, which are able to be enforced in practice.
  - Service providers should be required to notify oversight bodies of any instances of data security breaches.
  - A shorter maximum data retention period should be imposed and States should enjoy considerable leeway as to the minimum data retention period.

[39] Evaluation Report, note 1, p. 22.
[40] Shadow Report, note 29, p. 10.