Statewatch Briefing

Mandatory data retention in the EU

The drafting and subsequent implementation of the European Union's Data Retention Directive (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006) has been the subject of controversy and legal challenges.[1]

The Directive requires Internet Service Providers (ISPs) to retain data types of data from every communication made via any telecommunication device:

– landline phone
- fax
- mobile hones (including location of the call)
- and internet usage.

The Directive requires the collection and retention of:

- 'Internet Protocol (IP) address
- user ID
- phone number
- name, and address of every sender and recipient

but excludes the monitoring of content itself' – except for internet usage as the logging of the sites and pages viewed reveals the content of the communication.[2] Under the Directive communications data can be held for a minimum of six months and a maximum of two years. Which agencies and authorities should be given access to the data, and under what terms and conditions, is left to Member States to decide.

The legislation was opposed by a number of Member States as well as a large number of NGOs and individuals. It was passed with majority support in both the European Parliament and the Council. Implementation of the Directive, however, has not been a smooth process. Article 14 of the Directive requires that the European Commission submit to the European Parliament and the Council an evaluation of whether the articles dealing

---

[1] Directive of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC: http://www.statewatch.org/semdoc/assets/files/council/DIR-2006-24.pdf See also: Statewatch's Observatory on the Surveillance of Communications in the EU which covers the controversial adoption of the 2006 Directive: http://www.statewatch.org/eu-data-retention.htm

[2] Palfrey, John and Hal Roberts, 2010. 'The EU Data Retention Directive in an Era of Internet Surveillance' in Deibert, Ronald, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (USA: Massachusetts Institute of Technology), p.35

with the categories of data to be retained, and access to that data, should be amended in the light of its impact on 'economic operators and consumers', as well as technological developments. Considering the furore that has surrounded the Directive, it is expected the Commission would take into account the negative impact on individual rights, something well demonstrated by a number of cases that have been brought before national courts.

The first Member State to reject the provisions of the Directive (at least in part) was Bulgaria, when, following a legal challenge by the NGO Access to Information Program, the country's Supreme Administrative Court annulled an article of the legislation that attempted to transpose the Directive into Bulgarian law. This was due to the fact that:

"no mechanism was established for the respect of the constitutionally granted right of protection against unlawful interference in one's private or family affairs and against encroachments on one's honour, dignity and reputation."[3]

Furthermore, the provision attempted to provide various authorities with access to retained data 'for the purpose of the criminal process' and 'for the needs of national security', without providing reference to laws and constitutional rights in existence that regulate access to such data. Reference was also made to the provision violating Article 8 of the European Convention on Human Rights (ECHR).

Attempts to transpose the Directive into national law in Bulgaria's northern neighbour, Romania, met similar problems. The proposed national legislation was found to violate a number of articles of the Romanian constitution, namely those protecting freedom of movement, the right to intimate, private and family life, secrecy of correspondence, and freedom of expression. Article 8 of the ECHR was also invoked by the Romanian Constitutional Court in its judgement, along with Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, both of which forbid arbitrary interference with privacy, family, home or correspondence. Justifying the mandatory retention of data by invoking undefined "threats to national security" was found to be unlawful, as it meant that:

"some regular, routine actions of physical and legal persons may be appreciated, in an arbitrary and abusive way, as such threats".[4]

Germany's Constitutional Court also ruled against transposing the Data Retention Directive into national law. In a complaint brought by 35,000 citizens via the organisation Arbeitskreis Vorratsdatenspeicherung (AK Vorrat, Working Group on Data Retention), the court ruled that "such retention represents an especially grave intrusion into citizens' privacy", and that data already collected under the ruling should be deleted immediately. Nevertheless, the legislation was not annulled but instead was suspended.[5]

At the European level, a case brought before the European Court of Justice (ECJ) by Ireland in early 2009 that attempted to have the legislation annulled by appealing against the legal basis (Article 95 EC Treaty) of the Directive. It was argued that because Article 95 EC Treaty relates to regulating and enhancing the functioning of the internal market, it could not serve as a legal foundation for the Data Retention Directive, which was

[3] European Digital Rights, *Bulgarian Court annuls a vague article of the data retention law,* http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention

[4] Constitutional Court of Romania, *Decision No. 1258 from 8 October 2009,* http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

[5] AK Vorrat: http://www.vorratsdatenspeicherung.de/content/view/77/85/lang,de/#Evaluierung

introduced specifically for the purposes of fighting terrorism and organised crime. The court dismissed the case. While numerous paragraphs of the preamble of the Directive mention the usefulness of telecommunications data in combating crime and terrorism,[6] the ECJ ruled that 'the substantive content of its provisions… are essentially limited to the activities of service providers and do not govern access to data or the use thereof by the police or judicial authorities of Member States'.[7]

The NGO Digital Rights Ireland currently has another case pending at the ECJ; it is due to be heard this year. A judgment of the Irish High Court referred the following questions to the ECJ:

> Whether Directive 2006/24/EC is valid notwithstanding:
> (a) Article 6(1) and (2) of the Treaty on European Union ("TEU")
> (b) Article 3a TEU and 21 TFEU [Treaty on the functioning of the European Union] (formerly Articles 10 and 18 TEC)
> (c) Article 7, 8, 11 and 41 of the CFR [Charter of Fundamental Rights)
> (d) Article 5 TEU (formerly Article 5 TEC) (the principle of proportionality)

Although a previous case questioning the legal basis of Directive 2006/24/EC was dismissed by the ECJ, it noted at the time that its decision related solely to the question of the legal basis of the Directive, and 'not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy'.[8] The court's decision in this case could force the European Commission back to the drawing board in its attempts to enforce mandatory retention of all telecommunications data.

As well as leading the way in having the provisions of the Data Retention Directive scrutinised by national courts, NGOs have led an increasingly vigorous campaign to have it annulled at the European level in the name of protecting individual rights and finding less intrusive (and potentially more effective) ways to deal with the problems of terrorism and organised crime. A campaign was in place before the passing of the Directive and is still ongoing.

In late January 2011, a coalition of Romanian NGOs published an open letter demanding an end to data retention. In June 2010 over 100 representatives of organisations from across the EU published a letter that proposed the repeal of the Directive. A reply from Commissioner Malmström led to another letter arguing that blanket data retention is superfluous, harmful, and unconstitutional.[9] Indeed, it does not seem that the evidence is on the side of supporters of mandatory data retention. Statistics from the short period in Germany during which the retention of telephone and internet data took place demonstrate that although the number of crimes recorded increased, the number of crimes 'cleared' (e.g. through the bringing of charges) diminished in percentage terms.

In line with the Commission's obligation to evaluate the measure, and in light of the ongoing controversy surrounding the legislation, a conference was called in early

---

[6] See Paragraphs 5, 7, 8 10, 11, and 21 of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[7] European Court of Justice, *Judgement of the Court (Grand Chamber) of 10 February 2009 – Ireland v European Parliament, Council of the European Union (Case C-301/06),*

[8] European Court of Justice, Judgement of the Court (Grand Chamber) of 10 February 2009, Ireland v European Parliament, Council of the European Union (Case C-301/06), para. 57

[9] http://www.statewatch.org/news/2010/dec/eu-mandatory-data-retention-civil-society-letter-10.pdf

December 2010 'to finalise the evaluation of the Directive and to start the process of its review'.[10] It was here that Commissioner Malmström, apparently once a staunch opponent of mandatory data retention,[11] stated that 'data retention is here to stay'.[12] This u-turn is perhaps indicative of a strong institutional desire within the EU for mandatory data retention rules to remain in place. While the original Directive was passed under the UK presidency of the Council following the 2005 bombings of public transport in London, documents from 2002 demonstrate the desire of Europol to reach a 'common European Union law enforcement viewpoint on data retention'.[13] A number of countries - Austria, Greece, Ireland, the Netherlands, Poland, and Sweden - failed to implement the Directive by April 2009, as required by the legislation. In her speech to the December conference Commissioner Malmström stated that the Directive

"must… be implemented by all Member States. If necessary, the Commission will take action before the European Court of Justice to ensure that happens'.[14]

What you need to find out

1. Every EU Member State has to implement the Directive at national level. So the first job is to get a copy of your national law - and see how it compares with the Directive.

2. How has the Directive been implemented in your country? You need to make an FOI application to the government for the number of requests made by law enforcement agencies for access to communications data.[15]

Please provide me with data on how many requests for data have been made to communication services providers by law enforcement agencies since the approval of the law (i.e. transposition of the directive) in X country? Please provide this information broken down by year.

and

Do law enforcement agencies have direct, automated access to communications data held by service providers?

3. Under the Directive governments have to make a report to the European Commission on the national implementation of the Directive. This website has collected the response, so look and see if your country's response is listed: http://www.vorratsdatenspeicherung.de/content/view/77/85/lang,de/#Evaluierung

[10] http://www.dataretention2010.net

[11] In 2006 she stated that *"I have 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." See https://www.bof.nl/2010/12/08/data-retention-directive-evaluation-expect-the-unexpected/*

[12] Cecilia Malmström, speech to 'Taking on the Data Retention Directive' conference, December 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/723

[13] Statewatch, *Europol document confirms that the EU plans a "common EU law enforcement viewpoint on data retention*, http://database.statewatch.org/article.asp?aid=6427

[14] Cecilia Malmström, speech to 'Taking on the Data Retention Directive' conference, December 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/723

[15] In the UK in 2009 there were 525,130 requests – most of these were by law enforcement agencies who have automated access to service providers.