DATA RETENTION REVISITED

EDRi

EUROPEAN DIGITAL RIGHTS

European Digital Rights 12 Rue Belliard, 1040 Brussels www.edri.org @edri.org

Authors: Melinda Rucz, Sam Kloosterboer

Information Law and Policy Lab

Co-supervisor: Diego Naranjo, EDRi

This publication has benefited from the input of the EDRi network including Kristina Irion and Sarah Eskens from the Institute for Information Law (IViR), Rejo Zenger from Bits of Freedom, Jesper Lund from IT Pol Denmark, Romain Robert from noyb, Douwe Korff from fipr, Christiana Mauro from AK Vorrat and Walter van Holst from Vrijschrift.

Contents

Executive Summary

This report critically revisits the question of data retention, and concludes that the ongoing aspirations to reintroduce a data retention obligation in the EU remain in violation of EU law as long as the strict necessity of data retention is unproved and no genuinely targeted retention obligation is considered.

Following the judgments of the Court of Justice of the European Union in *Digital Rights Ireland* and *Tele2/Watson*, it appeared that the sun had set on blanket data retention in Europe. However, the data retention saga continues with renewed attempts to reinstate an EU legislative framework for blanket retention of telecommunications data. Data retention practices are highly privacy intrusive as they reveal vast personal, even sensitive, information about the persons whose data is retained. Retention of telecommunications data discourages the contacting of single purpose numbers and undermines the protection of journalistic sources. An inherently high risk of security breaches only amplifies these harmful effects of data retention, with numerous cyberattacks, data leaks, data abuses and misuses documented.

In light of the far-reaching negative implications of data retention for fundamental rights, the Court of Justice of the European Union has required data retention practices to be strictly necessary. Nevertheless, the necessity of data retention for law enforcement purposes is most often simply assumed, while evidence is lacking about the marginal benefits of data retention compared to less intrusive alternatives. Moreover, data errors, incorrect interpretations and false positives raise serious questions about the effectiveness of blanket data retention. The blind belief in the effectiveness of data-driven solutions manifests a worrying trend towards technological solutionism. While calls to reintroduce data retention often voice the need for harmonisation and legal certainty, enforcing the Court's judgments must be the default solution to ensure a harmonised approach to data retention in Europe. This report critically revisits the question of data retention, and concludes that the ongoing aspirations to reintroduce a data retention obligation in the EU remain in violation of EU law as long as the strict necessity of data retention is unproved and no genuinely targeted retention obligation is considered.

1. Back from the Dead: Data Retention in the EU

Mandatory retention of communications data by telecommunications providers has inspired significant privacy concerns in Europe. The EU Data Retention Directive, prescribing blanket retention of all communications metadata, sparked widespread controversy around Europe. According to the European Data Protection Supervisor (EDPS), the Directive was "the most privacy invasive instrument ever adopted by the EU".[1] In the seminal *Digital Rights Ireland* ruling, the Court of Justice of the European Union (CJEU) invalidated the Directive because of its privacy intrusive nature. In the subsequent *Tele2/Watson* decision, the CJEU confirmed that EU Member States may not impose an indiscriminate data retention obligation on telecommunications providers. In these cases, the CJEU has made clear that any data retention obligation is illegal unless the retention is targeted and is limited to what is strictly necessary in terms of the persons affected, the category of data retained and the length of retention. Regardless of the categorical condemnation of general data retention by the highest court of Europe, the issue of data retention continues haunting the agenda of political institutions of Europe.

As a report by Privacy International in 2017 reveals, EU Member States are reluctant to conform their national data retention practices to the requirements laid down in clear terms by the CJEU.[2] In 2017, the Council of the EU initiated a 'reflection process', "exploring options" to ensure the availability of communications data for law enforcement authorities. The reflection process has largely focused on the concept of 'restricted data retention', proposed by Europol. This envisages

1 European Data Protection Supervisor, 'The "moment of truth" for the Data Retention Directive: EDPS demands clear evidence of necessity' (3 December 2010), available at: https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2010-17_data_retention_directive_en.pdf.

2 Privacy International, 'National Data Retention Laws since the CJEU's Tele-2/Watson Judgment' (September 2017), available at: https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf.

the exemption of categories of data from the retention obligation that are "not even potentially relevant" for law enforcement, citing the length of the antenna or the number of ringtones as examples.[3] As the CJEU has ruled that it is unlawful to mandate the retention of data of people who are not even in a remote connection to serious crime, it is hard to see how 'restricted data retention' would pass the test. In May 2019, the Council concluded the reflection process, calling on the European Commission to consider a future legislative initiative on data retention.

In the meantime, negotiations continue on the revision of the ePrivacy Directive, protecting privacy and confidentiality of communications. The Council's reflection process has made clear the preference of Member States to establish a more favourable environment for data retention in the revised ePrivacy Regulation, foreshadowing the potential of introducing a data retention obligation through the back door.

Furthermore, the outbreak of the coronavirus crisis has triggered an increasing demand for telecommunications data to be shared with governments; and some have pointed to this tendency to call for a new harmonised data retention legislation of the EU.[4]

In light of the demonstrable attempts to bring data retention back from the dead, it is necessary to critically revisit the question. The European Commission has ordered a study for "possible solutions" for data retention in order to navigate its contemplation of a potential legislative initiative for a new data retention framework. The plans for this study have been partially published. Regrettably, as Digital Courage highlighted the study appears far from independent.[5] The plans reveal a biased focus on the needs and interests of law enforcement, and a lack of assessment of the impacts of data retention on the fundamental rights of European citizens. This report has been prepared to complement the study ordered by the Commission. It will critically assess the impact of data retention on fundamental rights and freedoms, evaluate the necessity and effectiveness of data retention and discuss threats posed by data retention such as misuse, abuse and data leaks.

3 Europol, 'Proportionate Data Retention for Law Enforcement Purposes' (September 2017), available at: http://www.statewatch.org/news/2018/feb/eu-council-data-retention-europol-presentation-targeted-data-ret-wk-9957-17.pdf.

4 For example: Patrícia Corrêa, 'Location privacy and data retention in times of pandemic and the importance of harmonisation at European level' (April 2020), available at: https://blogs.kcl.ac.uk/kslreuropeanlawblog/?p=1458#.Xtog6-dS82x.

5 Digital Courage, 'Blanket Data Retention: Biased Study the EU Commission' (March 2020), available at: https://digitalcourage.de/blog/2020/data-retention-biased-study-by-the-eu-commission.

2. Legal Framework

The Charter of Fundamental Rights of the EU (Charter) affords protection to the right to privacy and communications freedom in article 7, and the right to protection of personal data in article 8. According to article 52 of the Charter any limitation on the exercise of articles 7 and 8 must be provided by law, respect the essence of the rights and freedoms, genuinely meet an objective of general interest and satisfy a proportionality test. Charter rights that correspond to rights in the European Convention on Human Rights (ECHR) must be interpreted in accordance with the meaning and scope of the ECHR rights.[6] Article 8 of the ECHR safeguards the right to private and family life, which also encompasses the right to protection of personal data. The European Court of Human Rights (ECtHR) has invoked article 8 of the ECHR to condemn data retention practices in various cases and has consistently held that indiscriminate data retention constitutes an interference with article 8 ECHR.[7] The ECtHR's jurisprudence on data retention is an important guiding authority for the interpretation of the relevant Charter rights.[8]

EU legislative instruments have substantiated the protection of privacy and personal data. The ePrivacy Directive, aiming to protect privacy in the telecommunications sector, requires telecommunications data processed by telecommunications providers to be erased or anonymised as soon as it is no longer needed for the purpose of transmitting the communication or billing. Article 15(1) stipulates that Member States may allow for "the retention of data for a limited period", provided that such retention is "in accordance with the general principles of Community law" and constitutes a "necessary, appropriate and

6 Charter of Fundamental Rights of the European Union (2000) OJ C364/1, Article 52(3).

7 See e.g. S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, ECHR 2008 ; Roman Zakharov v. Russia [GC], no. 47143/06, ECHR 2015; Gaughran v. the United Kingdom, no. 45245/15, ECHR 2020.

8 The impact of ECtHR case law on the legality of data retention practices under EU law is discussed here: Franziska Boehm, & Mark D. Cole, 'Data Retention after the Judgement of the Court of Justice of the European Union' (2014) pp. 21-27, available at: https://www.zar.kit.edu/DATA/veroeffentlichungen/237_237_Boehm_Cole-Data_Retention_Study-June_2014_1a1c2f6_9906a8c.pdf.

proportionate measure" to safeguard "national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system".

The Data Retention Directive, adopted in 2006, obliged Member States to require telecommunications providers to retain all traffic and location data for a period between six months and two years. In *Digital Rights Ireland*, the CJEU invalidated the Directive because it infringed articles 7 and 8 of the Charter without such infringement being limited to what was strictly necessary. The CJEU problematised that the Directive did not lay down clear and precise rules in respect of the extent of interference caused by the Directive and it did not contain satisfactory safeguards in respect to access of the retained data by competent authorities.[9]

In *Tele2/Watson*, the CJEU reaffirmed its condemnation of "general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication".[10] The Court emphasised that any data retention legislation must lay down clear and precise rules and safeguards regarding the scope of the legislation so that the persons whose data is retained have "sufficient guarantees of the effective protection of their personal data against the risk of misuse".[11]

In its opinion on the envisaged EU-Canada PNR Agreement, the CJEU reiterated that the retention, access and use of personal data interferes with the right to privacy, regardless of whether the data is of sensitive nature or whether the person whose data is retained is inconvenienced in any way.[12] The Court once again emphasised the need for clear and precise rules regarding the conditions for retention, access and use of personal data, and the requirement of an objective link between the retained data and the objective of public security.[13]

9 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] paras. 60-62, 65.

10 Joined Cases C-203/15 and C-698/15 *Tele2/Watson* [2016] para. 134.

11 Ibid. para. 109.

12 Opinion 1/15 [2017] para. 124.

13 Ibid. paras. 190-192.

3. The Impact of Data Retention Practices on Human Rights

Data retention practices entail the storage of traffic and location data (metadata) by telecommunications companies for an extended period of time in order to ensure the availability of such data for law enforcement purposes. As electronic communications technologies are increasingly used in the course of criminal activity, electronic communications data can play an important role in criminal investigations.[14] Mandating the bulk retention of this data, however, poses serious risks to the right to privacy and communications freedoms. These risks are only amplified by the growing volume of electronic communications data as well as the sophistication of technologies recording such data.[15]

3.1 TWO LEVELS OF INTERFERENCE

Data retention practices interfere with the right to privacy at two levels: at the level of retention of data, and at the level of subsequent access to that data by law enforcement. The CJEU recognised in *Digital Rights Ireland* that the retention of communications data already constitutes an interference with the right to privacy.[16] This resonates with the stance of the ECtHR which held in *Marper v UK* that the mere retention of data interferes with the right to

14 See e.g. Council of the European Union, 'Europol Contribution to the Council Working Party on Information Exchange and Data Protection (DAPIX) Friends of Presidency' (11 May 2017), available at: https://www.statewatch.org/news/2018/feb/eu-council-data-retention-europol-data-to-be-retained-wk-5380-17-censored.pdf.

15 For example, the next generation of telecommunications systems, 5G, will be able to pinpoint location data with much more precision than previous systems, aggravating privacy risks of location data retention. See: Privacy International, 'Welcome to 5G: Privacy and Security in a Hyperconnected World (Or Not?)' (23 July 2019), available at: https://privacyinternational.org/long-read/3100/welcome-5g-privacy-and-security-hyperconnected-world-or-not.

16 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] para. 34.

private life, regardless of whether and how it is accessed later.[17]

In light of this, it is problematic that policy attention appears to be shifting from regulating storage of data to regulating access to retained data. It is increasingly argued that regulating access to retained data is sufficient to mitigate the interference presented by mandatory storage of communications data. For instance, Europol put forward that strict regulation of access to retained data should compensate for wide interference at the retention stage.[18] Such aspiration overlooks the intrusiveness of mere storage of communications data in bulk, clearly problematised by Europe's highest courts. Unless interference at both levels is strictly necessary and proportionate, the data retention practice remains illegal.

3.2 THE INTRUSIVENESS OF METADATA

Metadata, the object of data retention practices, is often seen as innocent and its storage harmless because it does not reveal the content of communications.[19] The intrusive nature of metadata, however, has been increasingly illuminated, underlying the stance of the CJEU that metadata "is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained".[20]

In Germany, a politician requested to access his location data stored by Deutsche Telekom under the former data retention legislation of Germany, and published the results on an interactive map. While the data points separately are insignificant, their combination gives a clear picture of his daily routine, his travelling habits and his preferences for pastime activities.[21] A Stanford University research, investigating the intrusiveness of telecommunications metadata, found that it is possible to infer romantic relationship status from call metadata. The study also concluded that it is possible to draw sensitive inferences about metadata: calls to religion-affiliated numbers can reveal religious attitudes, whereas calling specific health services might reveal medical conditions.[22] It has also been highlighted that when certain phone numbers are exclusively used for a single purpose, such as suicide hotlines or hotlines for victims of domestic violence, telecommunications metadata can be extremely revealing.[23] Subject lines of emails,

17 S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, para. 67, ECHR 2008.

18 Europol, 'Proportionate Data Retention for Law Enforcement Purposes' (18 September 2017), available at: https://www.statewatch.org/news/2018/feb/eu-council-data-retention-europol-presentation-targeted-data-ret-wk-9957-17.pdf.

19 This premise has often been voiced to justify the (by now invalidated) Data Retention Directive. See Elspeth Guild and Sergio Carrera, 'The political and judicial life of metadata: Digital rights Ireland and the trail of the data retention directive' (2014) 65 CEPS Liberty and Security in Europe Papers, p. 1.

20 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] para. 27; Joined Cases Joined Cases C-203/15 and C-698/15 *Tele2/Watson* [2016] para. 99.

21 Kai Biermann, 'Was Vorratsdaten über uns verraten' [What metadata reveals about us] (24 February 2011), available at: https://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz.

22 Jonathan Mayer, Patrick Mutchler and John C. Mitchell, 'Evaluating the Privacy Properties of Telephone Metadata' (2016) 113 Proceedings of the National Academy of Sciences 5536.

23 Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race and the Future of Law Enforcement* (NYU Press, 2019) p. 112.

also a type of metadata, are often telling of the content of emails.[24]

3.3 CHILLING EFFECTS ON FREEDOM OF EXPRESSION

The intrusive nature of data retention practices can induce chilling effects on the right to freedom of expression, which was recognised by the CJEU in both *Digital Rights Ireland* and *Tele2/Watson*.[25] Data retention practices might discourage the contacting of single purpose numbers as metadata about these calls could be extremely revealing, as discussed above. A German study from 2008 indeed found evidence for such effect: the majority of participants in the research reported that they would refrain from contacting a marriage counselling centre, a psychotherapist or a drug counselling centre because of the (former) data retention legislation.[26]

Data retention practices also threaten the ability of journalists to exercise their right to freedom of expression. Particularly investigative journalism, relying heavily on confidential sources, is jeopardised by indiscriminate data retention. Whistleblowers could feel discouraged to come forward because data retention practices could undermine traditional source protection measures.[27] While the CJEU has demanded that any data retention measure provides for an exception for communications protected by professional secrecy[28], the European Federation of Journalists has questioned how a vague exception for the protection of journalistic sources could be implemented in practice.[29] As a result, data retention practices continue to pose a risk to journalistic reporting and thus press freedom. As press freedom is under increasing pressure around Europe, the possibility that data retention legislation may be abused to further intimidate journalists must be seriously considered.

24 European Data Protection Supervisor, 'Pleading Notes of the European Data Protection Supervisor' (9-10 September 2019) p. 4, available at: https://edps.europa.eu/sites/edp/files/publication/19-09-11_data_retention_pleading_en.pdf.

25 Digital Rights Ireland para. 28; Tele2/Watson para. 101.

26 FORSA, 'Opinions of Citizens on Data Retention' (4 June 2008), available at: http://www.vorratsdatenspeicherung.de/content/view/228/79/.

27 UNESCO, 'Protecting Journalism Sources in the Digital Age' (2017) p. 24, available at: https://unesdoc.unesco.org/ark:/48223/pf0000248054.

28 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] para. 58; Joined Cases Joined Cases C-203/15 and C-698/15 *Tele2/Watson* [2016] para. 105.

29 European Federation of Journalists, 'German Journalists Oppose Data Retention Rules for Violating Professional Secrecy' (28 May 2015), available at: https://europeanjournalists.org/blog/2015/05/28/german-journalists-oppose-data-retention-rules-for-violating-professional-secrecy/.

4. Strict Necessity: Proven or Assumed?

On the basis of article 52(1) of the Charter, a limitation on the exercise to the right to privacy must be necessary and it must meet objectives of general interest recognised by the Union or the need to protect the rights and freedom of others, as these limitations are subject to the principle of proportionality. According to the CJEU case law, derogations and limitations in relation to the right to privacy may only be imposed if they are *strictly* necessary. In *Digital Rights Ireland*, the CJEU clarified that the interference with the right to privacy caused by the Data Retention Directive was not limited to what was strictly necessary. The CJEU furthermore confirmed the view of the ECtHR that mere usefulness does not satisfy the test of necessity.[30] In other words, the mere fact that data retention could be useful for law enforcement does not legitimise such a far reaching interference with the right to privacy.

In 2017, the EDPS published the Necessity Toolkit, elaborating on the requirement of necessity with respect to EU measures that interfere with the right to privacy and protection of personal data. It outlined that the test of necessity "implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal".[31] Moreover, the requirement of strict necessity, as developed by the CJEU, also implies strict judicial review, meaning that the legislator has limited discretion in choosing a measure when it constitutes a serious interference with fundamental rights.[32] In the Proportionality Guidelines, complementing the Necessity Toolkit, the EDPS clarified that the proportionality test requires that the

30 See: Silver and Others v. the United Kingdom, 25 March 1983, para. 97, Series A no. 61; Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke* [2010] para. 86.

advantages brought about by a measure are not outweighed by its disadvantages.[33] An assessment of proportionality, however, is only warranted if the measure has already satisfied the test of necessity.[34]

4.1 POLITICAL STATEMENTS DO NOT PROVE NECESSITY

While conclusively proving the necessity of data retention practices is inherently difficult, it is clear that mere political statements pointing to the value of data retention do not sufficiently substantiate the need for bulk retention of telecommunications data. It is striking that it is precisely these political statements that have been relied on to demonstrate the necessity of data retention practices. In 2011 when the Commission was asked to evaluate the Data Retention Directive and its necessity, the Commission concluded that most Member States consider data retention to be valuable, rather than providing genuine proof showing the added value of data retention practices.[35] In the Council's recent reflection process, a critical assessment of the necessity of data retention is again lacking, with the Council simply stating that data retention is important for the investigation of crime.[36] The plans for the new Commission study on data retention illustrate again that the necessity of data retention is simply assumed, rather than critically evaluated.

Mere political statements about the value of data retention are empty without tangible evidence showing the marginal benefit of data retention practices compared to existing alternatives. Mere political statements cannot suffice to demonstrate the necessity of data retention in a legal sense.

4.2 LESS INTRUSIVE ALTERNATIVES

Law enforcement authorities already have many investigative tools and resources at their disposal to investigate crime. To evaluate whether data retention is strictly necessary, it is essential to examine less intrusive alternatives that law enforcement authorities can rely on and assess whether these are sufficient for the fight against crime. If similar results can be achieved with less intrusive alternatives, data retention practices will remain illegal.[37]

Via the method of data preservation, also known as 'quick freeze', law enforcement authorities

31 European Data Protection Supervisor, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' (11 April 2017) p. 5, available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

32 Ibid. p. 7.

33 European Data Protection Supervisor, 'EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data' (19 December 2019) p. 9, available at: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

34 Ibid. p. 10.

35 European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)' (18 April 2011) p. 23.

36 Council of the European Union, 'Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime' (27 May 2019) para. 1, available at: http://data.consilium.europa.eu/doc/document/ST-9663-2019-INIT/en/pdf.

37 As held by the CJEU in *Schecke*: Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke* [2010] paras. 81-86.

can order telecommunications providers to store location and traffic data for a longer period if that data is of assistance in the investigation of a specific crime.[38] Targeted investigation techniques, such as the practice of data preservation, interfere with fundamental rights to a lesser extent as they do not place the entire European population under surveillance. However, some of the targeted investigation methods at the disposal of law enforcement authorities remain underexploited[39], whereas there is little proof that they are less effective in combating crime. In fact, studies have shown that law enforcement authorities investigate crime just as effectively with targeted methods as with blanket measures. A study conducted by the Max Planck Institute for Foreign and International Criminal Law in 2012 found that blanket data retention practices did not lead to higher crime clearance rates compared to less intrusive investigation methods.[40]

The EDPS already criticised the Commission in 2011 for failing to investigate less intrusive alternatives to data retention.[41] In light of this, it is striking that the Council's reflection process did not discuss alternatives to data retention, and the plans for the Commission's new study on data retention highlight that the study will not explore targeted investigation techniques. Without the evaluation of less intrusive alternatives and the demonstration of the net benefit of data retention compared to these alternatives, the strict necessity of data retention practices cannot be assessed and thus blanket data retention will remain illegal.

4.3 AVAILABILITY AND CONVENIENCE ARE NOT THE SAME AS NECESSITY

The availability of a vast amount of data to law enforcement authorities might create the false impression that data retention is necessary. The mere convenience of data retention for law enforcement authorities could incentivise law enforcement authorities to make use of data retention, instead of exploring their currently existing powers, such as accessing data upon a warrant, which is likely to be sufficient in most cases.[42] It is clear that these alternatives are less convenient for law enforcement. However, convenience is evidently not the highest or only priority when making an assessment of the necessity of such a privacy intrusive practice. The

38 See further: Elspeth Guild and Sergio Carrera, 'The political and judicial life of metadata: Digital rights Ireland and the trail of the data retention directive' (2014) 65 CEPS Liberty and Security in Europe Papers, p. 2.

39 As argued by Digital Courage, see (in German): Digital Courage, 'Scheinheilig: Regierungen und die Vorratsdatenspeicherung' [Hypocritical: Governments and Data Retention] (6 December 2019), available at: https://digitalcourage.de/blog/2019/scheinheilig-regierungen-und-die-vorratsdatenspeicherung.

40 Max Planck Institute for Foreign and International Criminal Law, 'Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten' [Security gap due to the absence of data retention? An investigation into security and law enforcement issues in the absence of telecommunications metadata storage] (July 2011), available at: https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf; For an English summary see: http://www.vorratsdatenspeicherung.de/content/view/534/79/lang,en/.

41 European Data Protection Supervisor, '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) paras. 53-57.

42 As already argued here: European Digital Rights Initiative, 'Shadow Evaluation Report on the Data Retention Directive (2006/24/EC)' (17 April 2011) p. 12.

mere convenience for law enforcement does not prove that data retention is a necessary tool for the prevention or investigation of crime.

4.4 VOLUNTARY DATA RETENTION

Telecommunications data that could be necessary for law enforcement authorities to investigate crime is currently already retained by telecommunications providers for their own business purposes, such as billing, fraud prevention, and individual network complaints.[43] Law enforcement authorities already have the power to demand access to this data upon a warrant. If the data may be relevant for ongoing investigations but it would be deleted too early, law enforcement authorities can order for the data to be preserved upon a 'quick freeze' request. The widespread practice of voluntary data retention casts further doubt on the necessity and marginal benefits of mandatory data retention. However, voluntary data retention for commercial practices also raises serious privacy concerns.

Although this form of voluntary data retention may in practice be less centralised and therefore perhaps less likely to be accessed by law enforcement authorities, it poses the same risks for individuals as mandatory data retention. In its case law, the CJEU views such commercial data retention as a restriction to the confidentiality of communications laid down in article 5(1) of the ePrivacy Directive.[44] As these are exceptions, they require a strict interpretation whether it concerns retention on the basis of recital 29 like billing, detection of technical failures in individual cases, or a restriction under article 15(1) like mandatory data retention.

The forthcoming ePrivacy Regulation will invariably add additional provisions for permitted processing compared to article 6 of the ePrivacy Directive which will potentially result in an increase of voluntary data retention. However, it must remain clear that these types of processing are regarded as exceptions to the confidentiality of communications and therefore demand a strict interpretation in accordance with CJEU case law.

The fact that telecommunication providers voluntarily retain a large amount of communications data for their commercial purposes raises questions about the additional need for mandatory data retention. Nevertheless, voluntary data retention also has severe adverse implications to the fundamental rights and freedoms of EU citizens, and thus the strict necessity of such voluntary retention must also be critically assessed.

43 See further on this point (in Dutch): Rejo Zenger, 'Zonder bewaarplicht wordt er nog altijd bewaard' [There is still retention without obligation] (23 March 2015), available at: https://www.bitsoffreedom.nl/2015/03/23/zonder-bewaarplicht-wordt-er-nog-altijd-bewaard/.

44 See e.g: Case C-119/12 *Probst* [2012] para. 23; Joined Cases C-203/15 and C-698/15 *Tele2/Watson* [2016] para. 89.

5. Issues with the Effectiveness of Data Retention Practices

Further casting doubt on the necessity of data retention practices, it has not even been proven if data retention is actually an effective way to combat serious crime. If the means are not an effective way to combat serious crime, the legislation cannot be necessary either. In its assessment of the Data Retention Directive, the Commission referred to data retention playing a "very important role" in criminal investigation and is sometimes "indispensable".[45] As pointed out by the EDPS, this argument is based on the view of a majority of Member States, which constitutes a desire rather than any proof that the data is an effective way to fight crime.[46] The plans for the new Commission study once again omit a critical evaluation of the effectiveness of data retention practices.

With data retention practices there is often an assumption that the retained data is first of all correct, and secondly leads to a correct outcome. However, there are various examples when telecommunications data is either inaccurate or false itself, or is incorrectly interpreted. Data errors, inaccurate interpretations and false positives raise serious questions about the effectiveness of data retention practices in the investigation of serious crime.

5.1 DATA ERRORS

In June 2019, it was revealed that incorrect telecommunications data served as evidence in more than 10 000 criminal cases in Denmark since 2012.[47] The data errors were caused by a flawed IT system that converted telecommunications data recorded by different providers into a uniform

45 European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)' (18 April 2011) pp. 23, 31.
46 European Data Protection Supervisor, '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)

format. Some data was lost during the conversion process, leading to incomplete call records. The system recorded location data incorrectly, sometimes resulting in errors of hundreds of meters. These severe errors mean that innocent people could have been incorrectly linked to a crime scene, whereas criminals could have been incorrectly excluded from investigations. In fact, 32 people were released from pre-trial detention due to the unreliable nature of location data as evidence in their cases.

Errors in how IP addresses are recorded have also led to wrongful arrests.[48] In order to convert IP addresses stored by telecommunications providers into useable evidence for law enforcement, they need to be manually retyped. As the British Interception of Communications Commissioner reports, errors in this process "are far more than acceptable".[49] This is especially true in the case of serious crimes, such as cases of child exploitation, where law enforcement errs on the side of speed rather than corroborating the accuracy of the evidence.

These data errors illustrate that the blind trust in the accuracy and objectivity of technological solutions is misplaced. This, in turn, not only casts doubt on the necessity and effectiveness of such a privacy intrusive practice as data retention, but also highlights the serious implications of data retention practices for the very foundations of a criminal justice system.[50]

5.2 FALSE POSITIVES

While it is often argued that blanket data retention is particularly useful when law enforcement has no suspects in a case, there is a clear risk that such use of data retention practices will lead to false positives. Location data recorded near a crime scene may wrongfully imply connection to the crime. In the United States, a man became a suspect in a criminal investigation merely because his smart phone location data was recorded near the scene of a burglary, as NBC News reported.[51] Relying on telecommunications data to 'fish' for suspects represents a fundamental shift in the way law enforcement authorities investigate crime, and risks undermining the principle of presumption of innocence.

47 See e.g.: Jon Henley, 'Denmark Frees 32 Inmates over Flaws in Phone Geolocation Evidence' (The Guardian, 12 September 2019): https://www.theguardian.com/world/2019/sep/12/denmark-frees-32-inmates-over-flawed-geolocation-revelations; Martin Selsoe Sorensen, 'Flaws in Cellphone Evidence Prompt Review of 10,000 Verdicts in Denmark' (The New York Times, 20 August 2019): https://www.nytimes.com/2019/08/20/world/europe/denmark-cellphone-data-courts.html.

48 Privacy International, 'IP Address Errors Lead to Wrongful Arrests' (2 January 2018), available at: https://privacyinternational.org/examples/1941/ip-address-errors-lead-wrongful-arrests.

49 Lisa Vaas, 'IP Address Errors Lead to Wrongful Arrests' (2018), available at: https://nakedsecurity.sophos.com/2018/01/02/ip-address-errors-lead-to-wrongful-arrests/amp/.

50 For example, the Minister of Justice of Denmark noted that the Danish scandal with the flawed telecommunications data has "shaken the trust in our legal system". Original statement available in Danish: https://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2019/nye-alvorlige-oplysninger-i-teledata-sagen.

51 Jon Schuppe, 'Google Tracked his Bike Ride Past a Burglarized Home. That Made Him a Suspect' (NBC News, 7 March 2020), available at: https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761.

5.3 A WORRYING TREND TOWARDS TECHNOLOGICAL SOLUTIONISM

Before any proposal is tabled to legitimise data retention practices, it is imperative to critically investigate its effectiveness in light of the potential of the aforementioned errors. The lure of technology cannot in itself justify the strive for data retention. Technology is not inherently correct, objective or more effective than non-technical solutions. However, exactly this assumption has long permeated discussions on the combating of security threats, and most recently also on the combating of the coronavirus crisis. Governments are exploring various digital tools as a strategy to manage the pandemic. The possible implementation of these digital strategies (mainly in the form of tracing apps) has led to much discussion on the effectiveness of these technologies and the impacts on privacy. Experts have warned to avoid a strategy based on "technological solutionism", which is the assumption that technology can solve any complex situation for humanity.[52] Apart from the possible implementation of tracing apps, the Commission has suggested to collect and analyse telecommunications metadata on a large scale to combat the virus.[53] However, the Commission has once again not proved that such data is actually a useful resource to combat the virus. In the case of tracing apps, experts have questioned the effectiveness as it is impossible to determine the proximity between individuals via Bluetooth and to draw correct conclusions about the possible transmission of the virus.[54]

In the case of telecommunications data, experts have mainly questioned the necessity of the use of such data. The Dutch legislator has proposed an amendment to the Telecommunications Act in order to legalise the collection and analysis of telecommunications data to combat the pandemic. However, the Dutch Data Protection Authority has warned that the necessity for this amendment has not sufficiently been demonstrated.[55] Moreover, the legislator has not discussed less intrusive alternatives, nor has it disclosed which specific data must be collected and for which objective. However, even before assessing the necessity of such an amendment, the legislator must prove that the use of telecommunications data is actually an effective means to combat the virus. In such an assessment, the risks of data errors or incorrect

52 See e.g.: Institute voor Informatierecht, 'New Project: Legal and societal conditions for Covid-19 technologies' (2020), available at: https://www.ivir.nl/new-project-legal-and-societal-conditions-for-covid-19-technologies/.

53 European Commission, ' Coronavirus: Commission adopts Recommendation to support exit strategies through mobile data and apps' (8 April 2020), available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_626. See also: Mark Scott, Laurens Cerulus & Laura Kayali, 'Commission tells carriers to hand over mobile data in coronavirus fight' (Politico, 25 March 2020), available at: https://www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-coronavirus-covid19/.

54 See e.g.: Maarten van Steen, ' Technische kanttekeningen bij een contact-tracingapp' [Technical comments on a contact-tracing app] (22 April 2020), available at: https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2020A01700.

55 Dutch Data Protection Authority, ' Advies over het conceptvoor wijziging van de Telecommunicatiewet in verband met informatieverstrekking aan het RIVM (Covid-19crisis)' [Advice on the draft amendment to the Telecommunications Act in connection with the provision of information to RIVM (Covid-19 crisis)] (19 May 2020), available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_telecomdata_corona.pdf.

interpretation must also be considered. For instance, individuals may drive through large parts of the country but stay within their vehicles. The analysis of their telecommunications data will falsely suggest that they have contributed to the dissemination of the virus to specific regions.

Although the use of telecommunications data to combat a pandemic necessitates a different balancing exercise than its use to combat serious crime, the approach by the Commission and national governments raises similar concerns. The Commission's eagerness to use telecommunications data and the assumption that this is an effective and necessary way to solve various problems, without exploring less intrusive alternatives, demonstrates a worrying trend towards 'technological solutionism'.

6. An Inherently High Data Security Risk

Data retention practices increase the potential for data security risks including data leaks, abuses and misuses. Evidently, the more data is stored, the more data can be abused or leaked upon a security breach. As telecommunications providers hold a vast amount of sensitive data, they are particularly attractive targets for complex and sophisticated cyber attacks.[56] Unauthorised disclosure of or access to retained telecommunications data considerably aggravate the privacy risks associated with data retention. This prompted the CJEU to require that any data retention measure provides for effective safeguards against abuse of and unlawful access to retained data.[57] It is important to note, however, that the retention of communications data is inherently sensitive to security breaches[58], regardless of the safeguards in place to prevent this.

6.1 CYBER ATTACKS

The latest annual report of the European Union Agency for Network and Information Security (ENISA) documented 157 significant security incidents in the telecommunications sector around the EU in 2018, and cyber attacks accounted for 5% of this (amounting to around 8 significant

56 See e.g. Mike Robuck, 'Telecommunications Industry Woefully Unprepared for Cyberattacks' (Fierce Telecom, 21 November 2018), available at: https://www.fiercetelecom.com/telecom/report-telecommunications-industry-woefully-unprepared-for-cyber-attacks.

57 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] para. 54; Joined Cases Joined Cases C-203/15 and C-698/15 *Tele2/Watson* [2016] para. 122; Opinion 1/15 [2017] para. 54.

58 As was already argued by Article 29 Working Party in 2010. Article 29 Data Protection Working Party, 'Report 01/2010 on the Second Joint Enforcement Action' (13 July 2010) p. 6, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp172_en.pdf.

security breaches).[59] Researchers at Cybereason discovered a large-scale global attack against telecommunications companies, stealing call records of specific 'high-value targets' from at least ten telecommunications networks.[60] In 2017, Spanish telecommunications provider, Telefonica, fell victim of a global ransomware attack.[61] While the impact of the attack was limited, it highlights the vulnerability of even large providers with sophisticated security safeguards in place.

6.2 ABUSE AND MISUSE BY AUTHORITIES

Beyond cyber attacks, there is also a risk that retained data is abused and misused by authorities. The mere availability of communications data may create an incentive for law enforcement to use it even when it is not strictly necessary. Cases where data retention legislation was abused to access journalistic sources have been well documented.[62] There is also a risk that retained data is used for purposes that are originally not envisaged by the legislation mandating such retention. For example, telecommunications metadata has been increasingly used for immigration control[63] or to combat the COVID-19 pandemic[64], normalising mass surveillance of telecommunications data beyond the boundaries of investigation of serious crime. Retained data that is available to law enforcement authorities is also available to secret services, making it hard (if not impossible) to track for what purposes it is used.

6.3 A HIGH PRICE TO PAY

These security risks are inherent in any data retention practice, regardless of the safeguards in place. As EDRi said in 2011, "only erased data is safe data".[65] The inherently high risk of security breaches is a high price to pay for any data retention practice which is clearly not offset by the marginal benefits it brings about, as the necessity and effectiveness of data retention for law enforcement purposes remains unproved.

59 European Union Agency for Network and Information Security, 'Annual Report Telecom Security Incidents 2018' (2019) p. 9.

60 Cybereason Nocturnus, 'Operation Soft Cell: A Worldwide Campaign Against Telecommunications Providers' (25 June 2019), available at: https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers.

61 Reuters, 'Telefonica, Other Spanish Firms Hit in "Ransomware" Attack' (12 May 2017), available at: https://www.reuters.com/article/us-spain-cyber/telefonica-other-spanish-firms-hit-in-ransomware-attack-idUSKBN1881TJ.

62 For example, a German and a Polish incident is mentioned in the report 'There is no such thing as secure data', available at: http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten_en.pdf.

63 See e.g.: Privacy International, 'Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers' (3 April 2019), available at: https://www.privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers.

64 See e.g.: Privacy International, 'Telco Data and Covid-19: A Primer' (21 April 2020), available at: https://privacyinternational.org/explainer/3679/telco-data-and-covid-19-primer.

65 European Digital Rights Initiative, 'Shadow Evaluation Report on the Data Retention Directive (2006/24/EC)' (17 April 2011) p. 8.

7. A False Appeal to Harmonisation

In the efforts to revive a European data retention legislation, it has been repeatedly emphasised that it is crucial to adopt a harmonised European data retention framework for the sake of legal certainty. Data retention obligations considerably vary across EU Member States, both in terms of their scope and their legal status. During the Council's reflection process, Europol argued that fragmented national rules hinder effective law enforcement, and thus urged the adoption of a harmonised approach to data retention, either as a new legislative act or through the revised ePrivacy Regulation.[66] The EU Counter-Terrorism Coordinator similarly suggested the adoption of a harmonised EU instrument on data retention, in order to establish a level playing field across the EU for all stakeholders.[67] The Council noted in its conclusions that the fragmentation of national data retention practices can cause limitations on law enforcement efforts, particularly in cross-border cases, and highlighted the necessity to provide for an EU regime on data retention.[68]

While the lack of harmonisation is indeed detrimental to citizens as well as telecommunications providers and law enforcement authorities, a one-sided focus on a new European data retention framework as a solution is misleading. Often an appeal to harmonisation is based on a faulty assumption that the current EU approach to data retention is unclear, fuelling uncertainty.[69] The CJEU has, however, laid down in clear terms what safeguards need to be implemented in order for data retention to be considered strictly necessary and proportionate. Adapting national data

66 Europol, 'Proportionate Data Retention for Law Enforcement Purposes' (18 September 2017), available at: https://www.statewatch.org/news/2018/feb/eu-council-data-retention-europol-presentation-targeted-data-ret-wk-9957-17.pdf.

67 EU Counter-Terrorism Coordinator, 'Data Retention: Contribution by the EU Counter-Terrorism Coordinator' (18 September 2017) p. 1, available at: https://www.statewatch.org/news/2017/nov/eu-council-ctc-working-paper-data-retention-possibilities-wk-9699-17.pdf.

68 Council of the European Union, 'Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime' (27 May 2019) paras. 5, 9, available at: http://data.consilium.europa.eu/doc/document/ST-9663-2019-INIT/en/pdf.

retention practices to the requirements enumerated by the Court would provide the desired harmonisation.

EU Member States have so far showed minimal political will to implement the Court's judgments, with many of them keeping illegal data retention laws. The general ignorance of the Court's judgments is also manifested in the Council's reflection process which has not put forward any suggestions for a data retention practice that is in any way targeted in terms of the persons affected. The European Commission, while legally required to ensure that the practices of Member States comply with EU law, appears unwilling to enforce the Court's judgments, and has refused to initiate infringement proceedings against Member States with illegal data retention practices. The plans for the new Commission study once again overlook this question: while it voices the need for a harmonised framework, it ignores the enforcement of the Court's judgments as a way to ensure harmonisation.

Under the pretext of harmonisation, Member States appear to strive to circumvent the Court's jurisprudence and legitimise blanket data retention, this way ignoring EU law. The push for data retention takes place at multiple levels: there are not only efforts to introduce a new EU data retention legislation, or afford a more favourable environment for data retention in the revised ePrivacy Regulation, but the CJEU is also facing political pressure to revise its judgments. Four cases are currently pending before the Court regarding data retention regimes in France, Belgium and the UK[70], posing similar questions to the ones the Court already ruled on in Tele2/Watson.

If a harmonised legislation on data retention is called for, it is for law enforcement authorities to demonstrate its marginal benefits compared to less intrusive alternative measures, as well as its proportionality, in light of the far-reaching negative implications on fundamental rights, exacerbated by inherently high security risks. Appealing to the need for harmonisation to support the introduction of a new data retention instrument is misguided, as enforcing the Court's judgments can similarly achieve harmonisation and is clearly the preferred solution in terms of respect for EU law. In his opinion on the pending cases, the Advocate General once again reiterated that general data retention is incompatible with EU law, and stressed that practical effectiveness is not the benchmark for national security measures, but instead legal effectiveness is, meaning respect for the rule of law and fundamental rights.[71] The ECtHR has recently also indicated its continuing condemnation of data retention practices; in Gaughran v UK it held that data retention without any safeguards breaches the right to private life.[72] As the highest courts of Europe repeatedly remind Member States that blanket data retention is illegal,

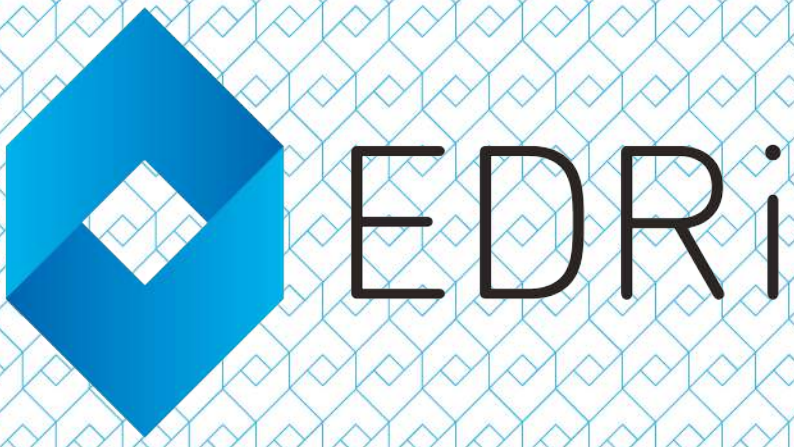
69 For example, the plans for the new Commission study on data retention note: "The invalidation of the Data Retention Directive and subsequent decisions of the CJEU have fuelled a degree of uncertainty amongst a broad range of actors" p. 3, available at: https://digitalcourage.de/sites/default/files/2020-03/200206%20Contract%20Data%20Retention%20Study%20Redacted.pdf.

70 Cases C-623/17, C-511/18 and C-512/18, and C-520/18.

71 Case C-623/17 *Privacy International* [2020], Opinion of AG Campos Sanchez-Bordona, para. 39.

72 Gaughran v. the United Kingdom, no. 45245/15, ECHR 2020.

Member States should not be allowed to sidestep their constitutional obligations. As long as the strict necessity of data retention practices is unproved, and no genuinely targeted data retention proposal is seriously considered, aspirations to bring data retention back from the dead will remain in contravention of EU law and the fundamental rights of over 500 million Europeans.



EUROPEAN DIGITAL RIGHTS

edri.org

@edri
brussels@edri.org