Mass data retention in the EU: time to break a bad cycle



EDRi
European Digital Rights

1. Why are you reading this?

In its 2025 internal security strategy "ProtectEU", the Commission announced the publication of an "impact assessment with a view to updating rules on data retention" at EU level.

"Data retention" is a legal requirement obliging providers of electronic communications services (e.g. telecom companies providing access to internet, email and private messaging) to retain certain types of data related to their users beyond what is necessary for the provision of their services and only for law enforcement purposes.

In 2014, the Court of Justice of the European Union (CJEU) invalidated the previous EU instrument (the Data Retention Directive) because it required a mass and indiscriminate retention of all traffic and location data, which the Court found to violate the Charter of Fundamental Rights.

Unfortunately, since then, the vast majority of Member States have ignored or circumvented the CJEU rulings and maintained illegal national data retention laws, which have been repeatedly challenged in court by digital rights organisations and service providers for violating EU law – **creating a never ending cycle, a harmful cat-and-mouse game**.

Rather than addressing this failure to comply with CJEU judgments, the European Commission is poised to introduce new EU legislation that could:

- **Legalise mass surveillance** at the European Union level
- **Undermine online privacy and other fundamental rights that depend on it** (freedom of assembly and association, of expression, etc.)
- Create **very serious cybersecurity risks** since all the data retained is vulnerable to increasing cyberattacks.

What we ask instead is the enforcement of EU law and the protection of people's fundamental rights and digital safety: **we recommend that the Commission prioritise launching infringement procedures against Member States whose data retention legal framework does not comply with the CJEU case law and bring all these infringing national laws into line with EU law.** This briefing explains:

- Why data retention matters more to your voters than you may think
- What metadata reveals about us
- What does the Court of Justice of the EU say about it
- Why extending the scope of an instrument which was already declared illegal is a bad idea.

2. Why does it matter to your voters?

Data retention is unpopular. Earlier attempts to institutionalise data retention have mobilised tens of thousands of people to protest against the proposed mass surveillance measures.



© fotos@queer-kopf.de

A 2025 consultation by the European Commission on its plans to harmonise EU data retention rules showed that the topic still resonates strongly with EU citizens. Around 96% of the respondents were EU citizens and, based on the contributions received, the vast majority of them opposed the Commission's plans and instead called on European policymakers to protect their privacy.

What do voters value? Summary of almost 5000 contributions

- **Politicians who respect their rights**: data retention is perceived as unwarranted mass surveillance and as placing the whole population under general suspicion. Respondents pointed out that they don't like to be treated like criminals and are worried that giving law enforcement such surveillance power will lead to abuses.

• **Protection against cybercrime and threats**: respondents pointed out that this is not just a matter of privacy, but data retention also creates security risks such as data breaches and exposure to stalking and identity theft.

• **Evidence-based policymaking**: many participants pointed out that the benefits of mass data retention for criminal investigations are limited and so far have not been proven with scientific evidence. Criminals will always find a way around and use services that minimise their exposure while others will have their right to privacy undermined.

• **Open-source and privacy-focused internet services**: data retention imposes a considerable economic and operational burden on service providers, which may ultimately be passed on to consumers, leading to increased prices for services and potentially stifling innovation within the digital market, especially from smaller, open-source and privacy-enhancing projects.

3. What does metadata reveal about us?

1. What is metadata?

Metadata is data generated for the purpose of transmitting content in electronic communications services and networks. It's the data about our use of communications: who communicates to whom, in what form, how often, for how long (if audio) or how big (if text) the communication is, from which (precise) geographic position it originates, from which phone number, with which subscriber identity, what the SIM card's IMSI number is, what the phone's IMEI (or "ID") is, etc.

It is also data about our "communications" with internet services/networks: the source IP address (as well as the IMEI and IMSI numbers), the domain name of the URL visited, the time and duration of the visit, the destination IP addresses, the frequency of visits. It doesn't include the content of the conversation (the voice or text message, the specific page viewed or what one typed or watched). Retained in bulk, metadata is the record about what every phone and computer (and their owner) does, all the time (including when it's just 'on' and the owner is not actively communicating – since devices 'communicate' all the time with the network, to ensure service reception).

1. CJEU, *C-817/19 Ligue des Droits Humains v Conseil des ministres*, 21 June 2022

2. Metadata reveals very intimate details of our lives

Metadata is very revealing about individuals' private lives. Since it's an immense collection of data points, it (perhaps counter-intuitively) reveals more than the content of the message itself would, as it makes it possible to:

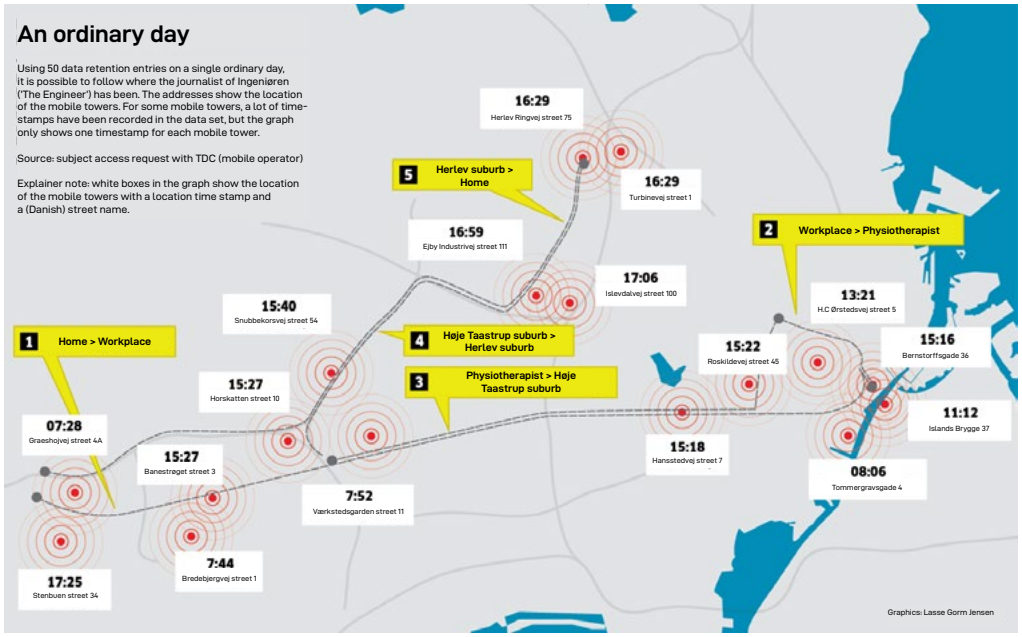
- Map a person's whole network of social and professional relations (a "social graph"), as well as the frequency, location and nature of their interactions.

- Map systematically the geographic location of a person over time, and to identify their permanent and temporary places of residence, their workplace, their visits to places that may reveal political and religious preferences (e.g. participation in public demonstrations and religious ceremonies), health status (e.g. visit to a specialised clinic), sexual orientation (e.g. LGBTQI+ venues), or other sensitive aspects (e.g. visit to a lawyer's office). It allows for the identification of the person's usual means of transport and routines, the school their children attend, etc.

- Shows what "online location" a person visits, and it's even more straightforward to reveal the person's sensitive data (concerning political and religious preferences, health status, sexual orientation, etc.) since it is often contained in the domain name of the websites and internet services visited. Metadata about internet services also easily reveals the person's usage patterns, which themselves invariably reveal an enormous amount of information about a person's interests and state of mind (e.g. how many times they visit the same website, at what time of the day, etc.).

In short, metadata reveals who you are, what you do, where you go, with whom you interact and what matters to you. It should therefore be treated with the same confidentiality and safeguards as content data (what we say to each other, which specific websites we visit and what we do/write/read/watch/share there).

3. Concrete example



Original: https://www.version2.dk/artikel/datatilsynet-truede-med-melde-tdcs-masseovervaagning-til-politiet
Translated by EDRi

4. What does the Court of Justice of the EU say about data retention? Summary of CJEU jurisprudence

Since the annulment of the Data Retention Directive (2006/24/EU) in the *Digital Rights Ireland* case of 2014, the Court of Justice of the European Union has developed its jurisprudence on data retention legislation in EU Member States.

The CJEU has consistently maintained that:

a) Articles 7, 8 and 11 of the EU Charter prohibit legislation which **mandates, as a preventive measure for combatting crime, the general and indiscriminate retention of traffic and location data by communications service providers.**

b) Traffic and location data enable the building of a very detailed profile of the individuals concerned, **information that is no less sensitive than the actual content of communications.**

c) **Retention of data and access to that data are separate interferences.** Whether the retained data is actually accessed is irrelevant for the assessment of the interference that retention of data constitutes. In fact, the legality of the retention requirement is a precondition for allowing access to the retained data.

d) **Access to retained data must be subject to strict safeguards.**

The following provides a summary of the most relevant judgements of the CJEU on data retention.[1]

1. 2014-2016: Mass data retention is prohibited by EU law

In the landmark cases, **Digital Rights Ireland (2014)** and Tele2/Watson **(2016)**, the CJEU established that general and indiscriminate retention of traffic and location data (metadata) for combatting serious crime is prohibited by EU law. The two judgements are based on the Charter of Fundamental Rights, and therefore apply to measures in both EU secondary law (the 2006 Data Retention Directive) and national law.

The CJEU also clarified that targeted data retention of traffic and location data is allowed by EU law. Such measures must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime. In this

1. The annex in the EPRS briefing "Mapping CJEU limits on data retention frameworks" has a detailed overview of all judgements from the CJEU and the European Court of Human Rights.

context, the CJEU highlighted geographical and person-based criteria (e.g. high-traffic areas or persons suspected of serious crimes).

2. 2020-2022: Type of data retention permitted by EU law

In La Quadrature du Net and others **(2020)** the CJEU delivered a comprehensive judgement which clarified the types of data retention permitted by EU law for a hierarchy of three purposes: (1) national security, (2) serious crime and (3) all criminal offences.

- For safeguarding national security against a serious threat that is shown to be genuine and present or foreseeable, the general and indiscriminate retention of all traffic and location data is permitted for a limited period. Data retention for national security cannot be systematic in nature.

- For combatting serious crime, only targeted retention of traffic and location data is compatible with EU law, as in previous judgements.

The CJEU did, however, make two clarifications to this rule:

1. General and indiscriminate data retention for combatting serious crime is permitted for **source IP addresses** for a period that is **limited in time to what is strictly necessary**. This was justified on grounds that the source IP address is less sensitive than other traffic data and that for offences committed online, there may not be other means of investigation.

2. **Civil identity data** can be retained in a generalised manner **for all criminal offences**, as this retention does not entail a serious interference.

In G.D. v Commissioner of An Garda Síochána **(2022)**, the CJEU clarified that access to retained data must be for the same purpose as the one justifying retention, or for a purpose of greater importance in the hierarchy. This is critically important, as it prevents Member States from using national security as a backdoor to general and indiscriminate data retention in criminal cases.

3. **2024: The specific case of source IP addresses**

In La Quadrature du Net and Others II **(2024)**, the CJEU provided further nuance (and legal complexity) on the retention of source IP addresses. General and indiscriminate retention of source IP addresses can be justified by the objective of fighting criminal offences in general, if the national law requires watertight separation between source IP addresses and other data. The underlying reasoning of the Court is that the watertight separation scheme puts retention of source IP addresses on an equal footing with retention of civil identity, insofar as interferences with fundamental rights are concerned.

However, the CJEU acknowledges that identifying a user from their IP address can constitute a serious interference, **where the context of the internet behaviour under investigation reveals more sensitive information about the individual**. In such cases, access to the retained data can only be granted for investigations of serious crime, and prior review by a court is required.

The only context in which the CJEU clarifies that source IP addresses do not 'typically' reveal such sensitive information is when it concerns a single copyright infringement. Although the Court does not assess other cases in its judgement, **it is clear that source IP addresses are typically connected to the context of the internet behaviour under investigation when law enforcement seeks to identify internet users**.

5. New scope of internet service providers = new range of problems

Since the 2000s, a significant share of digital communications has shifted from traditional telephone networks to internet-based services. This has prompted growing political interest in extending data retention obligations to cover these services. For example, in 2024, the High-Level Group (HLG) on Access to Data for Effective Law Enforcement recommended establishing a new EU data retention regime covering "present and future data handlers (i.e. Over-The-Top, OTTs, and service providers of any kind that could provide access to electronic evidence)".

Beyond the substantial legal concerns regarding data retention legislation, extending data retention obligations originally designed for telephone services to internet-based communications raises a number of distinct technical and legal challenges.

1. Definition

Number-independent interpersonal communications services (NI-ICS) do not connect to the public telephone network. Instead, they rely on the internet as their underlying technical infrastructure. They are often referred to as over-the-top (OTT) services because they are delivered "over the top" of an existing network infrastructure. Typical examples of NI-ICS include email services and messaging applications such as Signal and WhatsApp.

2. Evolution of the regulatory framework for NI-ICS

The annulled Data Retention Directive imposed data retention obligations on fixed-line and mobile telephone services (number-based interpersonal communications services), internet

access services and certain email services. Its scope reflected the definitions contained in the EU telecom regulatory framework (the "Framework Directive") and the ePrivacy Directive 2002/58.

Since December 2020, the European Electronic Communications Code (EECC) Directive has established a common regulatory framework for both number-based and number-independent interpersonal communications services. By extending the definition of electronic communications services to include NI-ICS, the EECC also brought these services within the scope of the ePrivacy Directive.

3. Challenges

A. Privacy-preserving by design

NI-ICS vary considerably in their technical architecture and in the extent to which they collect and process personal data. This contrasts with traditional telephone services, which are highly standardised through bodies such as ETSI and 3GPP. Some NI-ICS providers deliberately retain little or no data at all. This reflects a broader shift towards privacy-preserving design, driven by increased public concern following mass surveillance revelations, including those disclosed by whistleblower Edward Snowden, recognition of the benefits of anonymous communication, and the legal and commercial risks associated with storing personal data (e.g. data breaches). In practice,the ePrivacy principle that 'data which is not needed, is deleted' has become a widely accepted standard of digital hygiene.

B. Mandatory metadata collection weakens security

Some end-to-end encrypted (E2EE) services implement privacy-preserving features, such as "sealed sender", which technically prevent everyone – including the service provider itself – from monitoring who is communicating with whom.

Requiring providers to generate or make available metadata solely for the purpose of complying with data retention obligations, including targeted retention orders, would require fundamental changes to the design of these services. **Such changes would weaken the security architecture for all users, not only those subject to a specific investigation**. In this respect, a metadata retention obligation can be directly compared to a requirement to introduce an encryption backdoor to facilitate access to communications content: both reduce the security of all users and may fundamentally undermine the integrity of the service.

The distinction is legally significant. In 2024, the European Court of Human Rights (ECtHR) held, in Podchasov v. Russia, that legislation requiring the weakening of encryption for all users constitutes a **disproportionate interference with the right to privacy**. Although the judgment concerned access to the content of communications, the same legal reasoning arguably applies, by analogy, to the interception or retention of metadata, as the Court of Justice of the European Union (CJEU) has consistently recognised that traffic and location data are highly sensitive and capable of revealing detailed information about an individual's private life.

C. Global services cannot implement local retention obligations

Unlike traditional telephone services, which operate through nationally deployed physical infrastructure, many NI-ICS are provided on a global basis, often by companies established outside the EU. These providers may not be technically capable of implementing a data retention regime that applies only to a subset of their users, such as users located within a particular Member State or within the EU. At the same time, it is highly unlikely that providers would introduce a global data retention scheme in order to comply with a regional legal obligation.

Recent examples illustrate this change. In 2025, Apple withdrew its Advanced Data Protection service (end-to-end encrypted iCloud backups) in the UK instead of complying with a Technical Capability Notice requiring the company to facilitate access to the encrypted user data.

6. More resources

• European Parliamentary Research Service (EPRS), Mapping CJEU limits on data retention frameworks. A basic introduction, July 2025, https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775878/EPRS_BRI(2025)775878_EN.pdf

• European Parliamentary Research Service (EPRS), Analysis tailored for a member, General data retention / effects on crime, 27 January 2020, https://www.patrick-breyer.de/studie-strafverfolgung-funktioniert-ohne-vorratsdatenspeicherung/ - the study shows that there was no measurable effect of data retention regimes on crime rates or crime clearance rates in EU Member States.

• Eurojust and EJCN, The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU, November 2024, https://www.eurojust.europa.eu/sites/default/files/assets/files/data-retention-report-cjeu-eurojust-13-11-2024.pdf – the report shows that 12 Member States made key changes to their legislation between 2018 and 2022 in response to CJEU judgements (Prokuratuur and La Quadrature du Net and Others I), 15 Member States did not make any significant changes between 2018 and 2022, 3 Member States (EL, ES, CY) indicated that their current regulations are still based in essence on the invalidated Directive 2006/24/EC, 4 Member States have no data retention in place and 4 have attempted to introduce targeted data retention.

• Privacy International, PI's briefing on national data retention laws, 19 March 2024, https://privacyinternational.org/report/5267/pis-briefing-national-data-retention-laws

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us

Rue Belliard 12
1040 Brussels
Belgium

Follow us

Mastodon
Facebook
LinkedIn
Youtube
Instagram



EDRi
European Digital Rights