Submission to the European Commission's Call for Evidence for an Impact Assessment on Retention of Data by Service Providers for Criminal Proceedings

Submitted by the Electronic Frontier Foundation
June 18th, 2025

About the Electronic Frontier Foundation

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world.

Introduction and General Remarks

We welcome the opportunity to provide feedback on the European Commission's ('the Commission's') Call for Evidence for an Impact Assessment on retention of data by service providers for criminal proceedings. Any future measure in this area must start from ensuring the protection of fundamental rights, in particular the rights to privacy and data protection as set out in the Charter of Fundamental Rights of the European Union ('the Charter'), and must fully implement the binding jurisprudence by the Court of Justice of the European Union (CJEU).

Before responding to specific issues raised by the Call for Evidence, we want to recall the significant negative implications of data retention and the incompatibility of general and indiscriminate data retention with European law and the fundamental rights guaranteed under the Charter.

Societal Implications of Data Retention Requirements

Unfounded and indiscriminate data retention places all Europeans under general suspicion and erodes both anonymity and privacy. Proponents of data retention portray anonymity—online and offline—as a danger, whose primary functions are to provide cover for the commission of crimes. Consequently, it is assumed that anyone is a potential offender and must thus accept infringements of their fundamental rights in order to be identifiable in case of suspicion. However, it has been shown that the existence of surveillance increases the pressure to conform and leads to chilling effects on the exercise of freedoms protected by fundamental rights[1]. Similarly, privacy is considered a prerequisite for self-development, and the exercise of fundamental rights, including the rights to freedom of expression; freedom of thought, conscience and religion; free elections; and freedom of assembly and association.[2]As such, privacy and anonymity are essential elements of liberal democratic societies and necessary prerequisites for the full and uninhibited participation in society and democratic processes.

---

[1] Büscher, M., Hornung, G., Schindler, S., Zurawski, P., Gutjahr, A., Spiecker gen. Döhmann, I., ... & Wilmer, T. (2023). Abschreckungseffekte und Überwachungsgefühl im Datenschutzrecht: Auswirkungen auf betroffene Personen. *Datenschutz und Datensicherheit-DuD*, *47*(8), 503-512., Penney, J. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. *Regulation, and Chilling Effects Online: A Comparative Case Study (May 27, 2017)*, *6*(2).

[2] Wachter, Sandra (2017), *Privacy: Primus Inter Pares — Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights,* http://dx.doi.org/10.2139/ssrn.2903514

It is well established that metadata (traffic and location data) allows those with access to retained data to draw very precise conclusions about the lives of the persons affected, including their social relationships, physical movement patterns, and other elements of their private lives[3]. Knowing that someone communicates with a person offering specific services can be enough to draw incriminating inferences.

When every call record and IP log is retained and potentially accessed by law enforcement authorities, professional bearers of secrets, such as lawyers, doctors, therapists or journalists, cannot honor their obligations towards their clients, patients and sources.[4] When legal privilege and professional secrecy are compromised, vulnerable individuals forgo essential assistance, witnesses hesitate to testify, and journalistic informants are deterred from coming forward.

There is also evidence that once data is retained, unauthorized access to data and mission creep are serious risks. In the United Kingdom local authorities have relied on data collected under the Regulation of Investigatory Powers Act intended for combatting “serious crime” to pursue school truancy, littering, and dog fouling.[5] Similarly, Swedish enforcement authorities sought access to retained IP logs for routine copyright disputes under the IPRED framework, prompting Internet-service providers such as Tele2 to erase customer identifiers in protest.[6] In Ireland, a police officer exploited the country’s data retention system to obtain an ex-partner’s phone records[7].

Security Implications of Data Retention Requirements

Besides their negative societal implications, data retention requirements can also significantly contribute to cybersecurity risks. Mandatory data retention creates centralised troves of sensitive metadata, which in turn become high value targets for malicious actors. Rather than enhancing security, such measures often introduce new vulnerabilities. Retained metadata can reveal individuals’ contacts, movements, and behaviour patterns— information that, if leaked or breached, can be used for stalking, blackmail, discrimination, or other harms. Cyber attacks are on the rise and related losses reach up to 1.6% GDP in some EU countries[8]. One in five

---

[3] *Tele2 Sverige*, C-203/15 and C-698/15, para. 99

[4] See for example the CCBE *Recommendations on Client Confidentiality*, available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf

[5] Anushka Asthana (2016), *Revealed: British councils used Ripa to secretly spy on public*, available at: https://www.theguardian.com/world/2016/dec/25/british-councils-used-investigatory-powers-ripa-to-secretly-spy-on-public

[6] Kerstin Sjoden (200)*, Swedish ISP Thwarts Copyright Cops by Erasing Data*, available at: https://www.wired.com/2009/04/swedish-isp-thwarts-copyright-cops-by-erasing-data/

[7] Digital Rights Ireland (2011), *Garda who abused phone records to spy on ex will not be prosecuted, will keep job*, available at: https://www.digitalrights.ie/garda-who-abused-phone-records-to-spy-on-ex-will-not-be-prosecuted-will-keep-job/

[8] ENISA: “The cost of incidents affecting CIIs”, https://www.enisa.europa.eu/sites/default/files/publications/The%20cost%20of%20incidents%20affecting%20CIIs.pdf

businesses in the EU and US could face bankruptcy due to a cyber attack, and costs of dealing with attacks have recently increased by one-third[9]. Given this crisis of cyber security affecting European businesses, citizens and public administrations, the European Union cannot afford to create additional incentives for malicious actors by mandating the general retention of data.

Data protection and security concerns are amplified when retention is mandated for long periods and involves scaling up infrastructure to log and store user metadata that providers would otherwise delete. Forcing providers to retain IP addresses, subscriber identity, or geolocation data can compromise data minimisation, storage limitation, and privacy by design principles enshrined in the GDPR.

Illegality of General and Indiscriminate Data Retention Requirements

Beyond the negative societal implications of data retention mandates and associated cybersecurity risk, indiscriminate and general data retention has been found incompatible with European law and fundamental rights. The CJEU has ruled unambiguously that the general and indiscriminate retention of traffic and location data is incompatible with the Charter, regardless of whether such retention is enacted at the European or national level. In *Digital Rights Ireland*, the Court annulled Directive 2006/24/EC in its entirety, holding that it entailed a "wide ranging and particularly serious interference" with Articles 7 and 8 of the Charter, without such an interference being "precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary." (para 65).[10] The Court also found that the European legislature "has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter" (para 69).

These limitations were later reinforced in the *Tele2 Sverige* judgement, where the CJEU confirmed that "national legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, even when designed to combat serious crimes" (para. 107). The Court also held that "Article 15(1) of Directive 2002/58/EC, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication." (para. 112).[11]

The goal of harmonizing the currently fragmented landscape of data retention legislation in the European Union (EU) therefore cannot suffice to legitimize new general data retention requirements at the European level. Rather than proposing a new data retention mandate, the Commission should focus on aligning Member State's practices to the boundaries defined in

---

[9] HISCOX: *Cyber attacks strike insolvency fear into businesses,* available athttps://www.hiscoxgroup.com/news/press-releases/2022/16-05-22

[10] CJEU, *Digital Rights Ireland,* C-292/12 and C-594/12

[11] CJEU, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Watson and Others*, C-203/15 and C-698/15

CJEU case law. Several Member States continue to operate national data retention laws that violate the core principles of CJEU jurisprudence.[12]

EFF, therefore, urges the Commission to initiate infringement proceedings against Member States'' non-compliant legal national laws. We believe that any policy debate on data retention must be rooted in robust evidence and would only be meaningful once the jurisprudence of the Court uniformly respected across the EU.

Lack of Evidence Demonstrating Necessity for Blanket Data Retention

The Commission's Call for Evidence suggests that "the lack of harmonised data retention rules for key categories of data" presents "a substantial challenge" for national criminal proceedings and cross-border cooperation. Yet, it cites no empirical study, audit or statistics to justify that claim. Nor does it provide a systematic assessment of whether and how other, less intrusive investigative tools (such as targeted retention, quick freeze orders, or expedited cross border evidence production mechanisms) have failed to meet law enforcement needs.

Under Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms established by the Charter must be provided for by law, respect the essence of those rights, and be necessary and proportionate in light of a legitimate objective. The CJEU has consistently confirmed that interferences must be justified with evidence, and that general assertions of investigative utility are insufficient. For example:

- In *Digital Rights Ireland*, the Court held that "derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary" (para 52), and concluded that Directive 2006/24 imposed a "wide-ranging and particularly serious interference" with Articles 7 and 8 of the Charter "without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary" (para 65).
- In *Tele2 Sverige*, the Court confirmed that retention laws 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" (para 111). Earlier, it stressed that national rules authorising access must also comply with the principle of strict necessity (para 96).[13]
- In *Volker & Markus Schecke*, the Court found that the EU institutions had not "properly balanced" their transparency objective against the Charter rights at stake. Because "derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary" and it was "possible to envisage measures which affect less adversely" the right to privacy "and which still contribute effectively" to the EU's

[12] Privacy International (2024): *National Data Retention Laws*, available at: https://privacyinternational.org/report/5267/pis-briefing-national-data-retention-laws
[13] Text rectified by Order of 16 March 2017, OJ 2017 C 93/11.

> aims, the blanket publication rule "exceeded the limits which compliance with the principle of proportionality imposes" (para 86).[14]

These judgements confirm that anecdotal claims about the utility of general data retention do not satisfy Article 52(1). Hard, objective evidence is required.

The lack of data capable of demonstrating the need to access retained data for the purpose of combating crime is highlighted by the background document for the second plenary meeting of the High-Level Group (HLG) on access to data for effective law enforcement[15]. The document states:

> "Despite requests to this end, it appears unfeasible for law enforcement authorities to classify the criminal case types that are more or less reliant on access to data to be solved, as well as the categories of data which are necessary to investigate and prosecute criminal offences. National experts highlighted the difficulties faced in providing statistics which could quantify the importance of lawful access to data for successfully investigating and prosecuting crime, regardless of the type of offence suspected or the type of data required."

This confirms the findings of a 2012 study by the Max Planck Institute for International Criminal Law which found that no quantitative data on the usefulness of retained data existed, and that anecdotal qualitative evidence did not suffice to draw unambiguous conclusions on the effect of data retention mandates[16].

Lack of Evidence Regarding the Necessity of Retaining IP Address Data

Since the *Quadrature du Net II* (Hadopi) ruling in 2024, there is renewed interest in the blanket retention of IP addresses for the purpose of combating crime. The Commission's Call for Evidence suggests that the retention of IP addresses should be considered as a less controversial category of data to retain, while promising advantages for law enforcement authorities. However, the German Federal Criminal Office itself has concluded that the current practice of many providers to store IP addresses for seven days is sufficient to solve around three quarters of relevant cases[17]. This underlines the lack of necessity to introduce new, blanket mandates for the retention of IP address data.

---

[14] *Volker und Markus Schecke GbR*, joined cases C-92/09 and C-93/09.
[15] Input to the second plenary meeting of the High-Level Group (HLG) on access to data for effective law enforcement, 21 November 2023, available at: https://home-affairs.ec.europa.eu/document/download/05963640-de76-4218-82cd-e5d4d88ddf96_en?filename=HLG-background-document-21112023.pdf (page 2)
[16] Albrecht, Hans-Jörg (2012): *Schutzlücken nach dem Wegfall der Vorratsdatenspeicherung,* available at: https://static.mpicc.de/shared/data/pdf/schutzluecken_vorratsdatenspeicherung_12.pdf
[17] Bundeskriminalamt (2023): *Bedeutung der IP-Adresse in der Bekämpfung des sexuellen Missbrauchs von Kindern und Jugendlichen*, available at: https://cdn.netzpolitik.org/wp-upload/2023/06/2023-06-21_BKA_Bedeutung-IP-Adresse.pdf#page=7

Global Increase in Data Availability

Additionally, the overall availability of data has increased exponentially. The predominant business model of tech companies, including the online advertising and AI industries, relies on the collection and processing of data at a massive scale. This commercially collected data is increasingly accessed by law enforcement authorities. Last year's SIRIUS report on the electronic evidence situation in the EU[18] shows that social media data was considered the most relevant source of data for criminal investigations. To access this kind of data, investigators relied on direct requests to service providers. The volume of data disclosure requests has been increasing for years, with a 22% increase from 2022 to 2023 alone. This shows that law enforcement authorities have more access to data than ever before, further questioning the need for data retention requirements.

To address this lack of evidence necessary to demonstrate the lawfulness and proportionality of general and indiscriminate data retention obligations, we call on the Commission to include, at a minimum, the following information in any upcoming impact assessments:

- A detailed inventory of cases allegedly impacted by lack of retained data;
- Clarifications of what types of data were unavailable and whether alternative tools (e.g., quick-freeze, targeted preservation) could have been used;
- Detailed assessments of whether any proposed measure can be implemented without replicating the structural flaws that led to the invalidation of Directive 2006/24/EC;

Absent such a demonstration of necessity, the reintroduction of general and indiscriminate data retention obligations would violate settled CJEU jurisprudence and undermine the fundamental rights guaranteed by the Charter.

Retaining Data and Accessing Retained Data Constitute Separate Interferences Requiring Independent Justification

The CJEU has consistently clarified that the retention of personal data and the access to that data by competent authorities are distinct legal acts, each of which constitutes an interference with the fundamental rights to privacy and data protection under Articles 7 and 8 of the Charter. As such, each act must be assessed separately and must satisfy its own legal requirements of legality, necessity, and proportionality under Article 52(1) of the Charter.

In its judgment in *Tele2 Sverige*[19], the Court found that retained metadata is capable of revealing highly sensitive insights into an individual's private life, including movements, contacts, activities, and associations (para 99). It concluded that the interference entailed by such legislation is "very far-reaching" and "must be considered to be particularly serious", even where access to the data has not occurred (para 100). The Court further held that national legislation

[18] SIRIUS EU Electronic Evidence Situation Report 2024, available at: https://www.eurojust.europa.eu/sites/default/files/assets/files/sirius-e-evidence-situation-report-2024.pdf
[19] *Tele2 Sverige,* C-203/15 and C-698/15.

imposing data retention obligations must lay down clear and precise rules, including when and under what conditions retention is permitted, and must be subject to "minimum safeguards" to protect against misuse (para 109). The retention measure, therefore, requires an independent legal assessment under the Charter.

In a separate part of its analysis, the Court addressed the conditions governing access. It held that access to retained data must be limited to the objective of combating serious crime, must comply with the principle of strict necessity, and must be subject to clear substantive and procedural safeguards. Specifically, the Court required that access

- must correspond "genuinely and strictly" to one of the objectives listed in Article 15(1) of Directive 2002/58 (para 115),
- must "not exceed the limits of what is strictly necessary" (para 116), and
- must be governed by "clear and precise rules" and be legally binding under national law (para 117).

These findings affirm that retention of data and access to retained data are subject to independent legal tests. In a subsequent ruling, the Court has confirmed that access to retained data may only be lawful if the data has been retained in a manner that is consistent with Article 15(1) of the ePrivacy Directive[20]. Thus, the presence of access safeguards, such as judicial authorization or limitation to serious crime cannot cure the illegality of a general and indiscriminate retention obligations that are in violation with the ePrivacy Directive and fail to meet the Charters' standards.

The recent *La Quadrature du Net II* ruling does not depart from the Court's previously established principles regarding the access to retained data. While the judgment permits the accessing of retained IP addresses for the purpose of combating criminal offenses, the Court assesses that the retention of IP addresses is not a serious interference if national law mandating such retention assures that no precise conclusions about the private life of the persons affected can be drawn. This means that the retention of the data must be organized in such a way that any combination of those IP addresses with other data, retained in compliance with Directive 2002/58, would have to involve the watertight separation of data categories.[21]

We therefore call upon the Commission to treat retention and access as two distinct interferences, each of which must be separately evaluated in light of the European law, the Charter and CJEU case law. To do otherwise would risk repeating the fundamental rights violations that led to the annulment of the Directive 2006/24/EC and the invalidations of several national regimes that followed.

[20] *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, para 167.
[21] *La Quadrature du Net and Others*, C-470/21, paras 79 - 84.

Data Retention Requirements for Number-Independent Interpersonal Communications Services

The work of the High-Level Group (HLG) on access to data for effective law-enforcement and the Commission's Call for Evidence signal an interest in extending retention duties to number-independent providers of electronic communications services. Since the entry into force of the Interim Regulation on a temporary derogation from certain provisions of the ePrivacy Directive, providers of number-independent electronic communications services fall under the regime of the ePrivacy Directive. In the following, these providers are referred to as NI-ICS (number-independent interpersonal communication services).

So far, the Court has not ruled on data retention by NI-ICS specifically. However, nothing in *Digital Rights Ireland, Tele2 Sverige, La Quadrature du NetI* or *La Quadrature du Net II*[22] suggests that fundamental rights would be less protected in instances in which traffic is routed over the internet rather than the public switched telephone network (PSTN). Thus, irrespective of the transport layer, it should be assumed that any general and indiscriminate data retention obligations for NI-ICS would be unlawful under the ePrivacy Directive, the Charter and would be in collision with the according to the established jurisprudence of the Court.

NI-ICS encompasses a broad spectrum of providers, ranging from global providers to small, privacy focused European competitors. In practice, this category covers a range of different services, many of which are end-to-end encrypted privacy-preserving by design, opting to collect as little user data as possible. Thus, forcing NI-ICS to bulk retain user data would violate the GDPR: Articles 5(1)(c) and 25 of the GDPR impose a positive duty on data controllers to avoid the unnecessary collection and retention of data. Forcing NI-ICS to build new data collection and retention infrastructure would directly contradict these obligations and erode the security guarantees users, business and public administrations depend on.

Extending data retention requirements on NI-ICS would also undermine security and encryption. A number of end-to-end encrypted NI-ICS employ anonymity-by-design technologies to collect as little metadata as possible. Technologies such as "sealed sender" encrypt metadata and prevent even the service provider from knowing who communicates with whom. Extending data retention obligations to NI-ICS would force such services to either pull out of markets with such obligations, or risk non-compliance. Applying pressure to privacy-focused, end-to-end encrypted services to undermine encryption or collect data they services is not designed to collect, would compromise their user's security and the rights to privacy, data protection and other fundamental rights established by the Charter.

In a significant decision regarding application no. 33696/19 (*Podchasov v. Russia*)[23], the European Court of Human Rights (ECtHR) held that "the statutory obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such

[22] *La Quadrature du Net II,* C-470/21
[23] *Podchasov v. Russia*, application no. 33696/19, available at https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-230854%22]}

services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued"[24]. While this particular ECtHR ruling focused on technical backdoor measures for intercepting electronic communication content, the underlying principles are highly relevant to the bulk retention of connection or routing data. This is because both the CJEU and the ECtHR have previously stated that metadata can create a detailed portrait of an individual's private life, and thus attracts the same high level of protection as content.

Finally, we want to underline that the narrow carve-out by the *La Quadrature du Net II* case did not create a suitable template for data retention obligations extended to NI-ICS. *La Quadrature du Net II* sets out a three limb, cumulative test that any national law would have satisfy before any general and indiscriminate retention of source-IP addresses can be ordered: As stated above, national legislation must require (i) that each data category is retained in a separate, technically isolated silo, that any linking between silos occur only through a controlled mechanism; the arrangement must be so "genuinely watertight" that no combination of those datasets can ever reveal a detailed picture of a user's private life; (ii) that retention is ordered only for a period not exceeding what is strictly necessary and under rules that guarantee effective safeguards and that (iii) once HADOPI (or an equivalent body) has issued two warnings, the graduated-response process must pause; the body may not "link the civil identity data of a person (...) with the file relating to the work made available on the internet" because doing so "may (...) enable precise conclusions to be drawn about the private life of that person." Therefore "a prior review by a court or an independent administrative body (...) must take place before sending the third-stage notification" and only if that body "authorises that linking."[25]

As EDRi has stressed, these concessions are highly contextual: "These arguments about potentially sensitive information being strictly contained can be seen as "tailor-made" to the HADOPI system. This also means that they will not necessarily apply to other types of investigations."[26]

Therefore, *La Quadrature du Net II* does not (i) compel a provider that does not collect a given data category (or deletes it within hours) to build a new database; (ii) force the dismantling of privacy protective architectures; or (iii) authorise the retention of richer metadata sets that enable behavioural profiling. Thus, using the ruling as a template for mandatory IP data retention or for extending data retention requirements to NI-ICS would over-extend its legal reasoning and collide with the Court's jurisprudence on indiscriminate retention.

In summary, a mass-retention mandate for NI-ICS would violate settled CJEU doctrine, conflict with the GDPR, weaken Europe's security posture, and jeopardise trust in privacy-by-design innovation, without a demonstrable, evidence-based benefit for criminal investigations.

---

[24] *Podchasov v. Russia*, application no. 33696/19, para. 70, 79.
[25] *La Quadrature du Net II,* C-470/21, para 141.
[26] Chloé Berthélémy & Jesper Lund (2025), *CJEU saved the HADOPI: what implications for the future of data retention in the EU?*, available at https://edri.org/our-work/cjeu-saved-the-hadopi-what-implications-for-the-future-of-data-retention-in-the-eu/

Conclusion

The imposition of general and indiscriminate data retention requirements fundamentally subverts the presumption of innocence. Surveillance in the form of data retention has been demonstrated to erode established privileges of professional secrecy bearers, undermine press confidentiality, and diminish the essential privacy requisite for unfettered thought, free association, and the functioning of a liberal democratic society. There is no evidence to show that indiscriminate data retention mandates enhance public safety. On the contrary, they introduce new attack surfaces for malicious actors and foster an environment conducive to mission creep by domestic authorities.

This matter has been exhaustingly litigated: Directive 2006/24 and its transpositions into Member States' national laws were struck repeatedly. Each judgment re-affirmed the same principle in the context of criminal investigations: Only targeted and strictly necessary retention, bounded by robust, independent safeguards, can survive Charter review. The goal of harmonizing the currently fragmented landscape of European data retention laws does not resolve the incompatibility of indiscriminate data retention mandates with European law and fundamental rights.

The European Commission should therefore abandon any proposal for indiscriminate or quasi-indiscriminate retention, focus on enforcing existing Charter-compliant standards, and invest in evidence-based, targeted quick freeze measures that respect both security, fundamental rights and the presumption of innocence.