Centrum für Europäische Politik
FREIBURG | BERLIN

cepAdhoc

No 5 | 2025 11 March 2025

Security and Trust: An Unsolvable Digital Dilemma?

Europe Must Resist Weakening Encryption for Law Enforcement

Anja Hoffmann, Anselm Küsters, Philipp Eckhardt

Source: DALL-E prompt.

While police chiefs and governments claim encryption hinders access to vital evidence in cases of terrorism, child exploitation, and organised crime, experts warn that mandating backdoors or weakening standards threatens cybersecurity, human rights, and trust in digital infrastructure. A new EU internal security strategy, due at 1 April 2025, is likely to set the direction for the coming years. We argue that sacrificing digital privacy protections would create systemic risks that far outweigh any potential investigative benefits.

- Recent legislative pushes such as the UK's Investigatory Powers Act, Sweden's "non-paper" advocating mass surveillance, and EU debates on encryption threaten to normalise disproportionate state access to private communications. Controversial proposals to reintroduce sweeping data retention laws – previously struck down by EU courts – demonstrate the inherent tension between security and civil liberties in the digital age.
- Technical analyses confirm that weakening encryption cannot be narrowly targeted, creating vulnerabilities exploitable by malicious actors. Meanwhile, alternatives exist: law enforcement already leverages metadata, open-source intelligence, and platform-level content moderation tools without compromising encryption.
- Accordingly, weakening encryption is a false solution to complex policing challenges. By advocating for "security by design", funding more specialised research on rights-respecting methods, and rejecting flawed compromises, Europe can uphold its commitment to privacy. Moreover, the complexity of the topic requires more meaningful and representative input from all sides: Member States, service providers, and civil society.

Content

1 Introduction

While digitalisation has improved the way people communicate and do business, it is often forgotten that it also creates new challenges for law enforcement. Security officials and police are increasingly relying on the ability to access electronic data to prevent, investigate, and prosecute crime. For several years now, the European Union (EU) and its Member States have been asking themselves how to ensure that essential security measures remain effective in the digital environment without undermining the fundamental rights, privacy, and trust that underpin democratic societies.

To give a recent example of this important but often ignored debate, the UK government recently escalated its efforts to gain access to encrypted data by demanding that Apple create a backdoor to its cloud storage system.[1] The request, made under the Investigatory Powers Act (IPA), would force Apple to provide access to encrypted backups stored by users around the world. Currently, Apple's Advanced Data Protection (ADP) ensures that only account holders can access their own encrypted cloud data, preventing even Apple itself from viewing the content. Privacy advocates warn that creating such a backdoor would set a dangerous precedent, as any method that allows UK authorities to access encrypted messages could also be exploited by foreign governments or cybercriminals. Critics were also alarmed to discover that this law's extraterritorial reach would effectively allow UK authorities to access the encrypted iCloud data of any Apple customer worldwide.[2] In other words, this heavy-handed approach would have compromised the security of users everywhere, sparking significant backlash from industry and privacy groups alike. In response, Apple has now announced that it will simply withdraw its ultra-secure end-to-end encryption for iCloud in the UK, rather than comply with the demands. The company insists it has never built a "backdoor" or "master key" and claims it never will.

The Apple-UK dispute has raised concerns and grabbed media headlines, including via an intervention by Donald Trump[3], but it is just one example of a wider issue concerning the potential impact of digitisation, encryption, and security requirements on global digital privacy and security. With the incoming European Commission, the debate on the proper balance between security needs and the protection of personal data is now reopening in Europe. In its recently published work programme, the Commission announced a new "European Internal Security Strategy" to be presented 1 April 2025.[4] While the strategy shall include "a comprehensive set of actions", digital technologies shall play a substantial role, too. As mentioned in a "call for evidence", the Commission wants, without going into further detail, to "consider measures on access to data for law enforcement and data retention, fighting cybercrime and terrorist content online, and boosting cooperation with tech platforms via the EU Internet Forum".[5] The wider debate is taking place in the context of a political shift to the right across much of Europe, raising the stakes for the next Commission's policy agenda in the field of Justice and Home Affairs. In July 2024, a leaked Swedish government paper called for a "fundamental change of perspective" in the fight against terrorism and organised crime, arguing that too many proposals were watered down by fundamental rights considerations.[6] At the 2025 World Economic Forum in Davos, Europol's

---

1 For the background, see: Kleinman (2025), UK government demands access to Apple users' encrypted data, BBC.

2 Bradshaw and Fisher (2025), Apple withdraws cloud encryption service from UK after government order, FT.

3 In an interview with the British magazine "The Spectator", Trump clearly criticized the British government. He said that such an approach was only known from China and that it could not be done this way [https://www.spectator.co.uk/article/trump-uk-encryption-laws-are-like-what-you-get-in-china/].

4 European Commission (2025), 2025 Commission work programme.

5 European Commission (2025), Call for evidence - Ares(2025)1157428, European Internal Security Strategy.

6 See: Statewatch | Police should have "more say in the EU policy-making process," says Swedish government.

executive director, Catherine De Bolle, has even assigned Big Tech companies such as Meta, WhatsApp, and Signal a "social responsibility" to give law enforcement full access to encrypted messages for criminal investigations.[7]

In the remainder of this cepAdhoc, we explore some key aspects of how to reconcile law enforcement's legitimate need to access data with the EU's fundamental rights obligations. By way of context, section 2 explains key concepts and traces the EU debate on encryption and law enforcement. Section 3 then focuses on the tangible risks of compromising encryption, drawing on game-theoretical analyses, while section 4 looks across the Atlantic to show how recent developments in the US illuminate the broader security implications of weakening privacy safeguards. Section 5 presents alternative solutions for designing a framework that addresses law enforcement concerns without undermining digital security and personal privacy. Finally, Section 6 concludes with a forward-looking perspective on what upcoming EU initiatives could mean for the design of proportionate, harmonized, and rights-compliant data access policies. As EU policymakers draft and agree on the new Internal Security Strategy and the Digital Networks Act, they must ensure that legitimate public safety objectives do not undermine the trust and security that are essential to both fundamental rights and a robust digital economy.

2 Background: EU security policy in the digital age

Encryption is the process of converting readable data into scrambled, unreadable code using mathematical algorithms and cryptographic keys, ensuring only authorized parties can access the original information.[8] In today's digital environment, encryption manifests in four key forms: symmetric (single shared key requiring secure distribution), asymmetric (public-private key pairs enabling one-way security), end-to-end (E2E, ensuring only sender/recipient access with services excluded), and data-at-rest (protecting stored digital information).[9] While symmetric encryption prioritizes speed and asymmetric systems enhance security by eliminating key transfer risks, E2E protocols like Signal or PGP uniquely safeguard communications from third parties – including service providers – by design. Layered approaches (e.g., encrypting emails via PGP and HTTPS transmission) compound protections, yet metadata (sender, timestamps, etc.) often remains exposed even in encrypted systems.

The tension between preserving robust encryption and maintaining law enforcement capabilities has long been at the heart of EU policy discussions.[10] Since 2002, the EU ePrivacy Directive (2002/58/EC)[11] requires Member States and businesses to ensure the confidentiality and security of their communications, related networks and services. Updated in 2008, it provides that any interference with electronic communications, including encryption, must be necessary, proportionate, authorized by law and subject to adequate safeguards. The call to strengthen the fight against serious crime and terrorism using interception and decryption of electronic communications already came up in 2010. Since then,

---

7 See: Europol chief says Big Tech has 'responsibility' to unlock encrypted messages, FT.

8 See: What is encryption? | IBM.

9 See: Policy Brief: Encryption - Internet Society.

10 For a summary of the prehistory, see: Chousou, S./Magaud, J./Pavoni, L/Williams, M. 2023. "Is encryption a fundamental right? A case study on CSAM regulation in the EU". Sciences Po, Section 3, https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/07/Encryption.pdf.

11 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

further developments have resulted in two major European debates on encryption[12]: the first one on the prevention of terrorism, and the second one on an EU Strategy for a more effective fight against child sexual abuse.

In June 2017, the European Council expressed concerns about systems that allow terrorists to communicate beyond the reach of investigating authorities, including end-to-end encryption, and called to address the related challenges. At the same time, it underlined the importance of safeguarding privacy and data protection, as well as the overall benefits of these systems. Recognising that effective access to electronic evidence is "essential to combating serious crime and terrorism", the European Council demanded that the availability of data be ensured, subject to appropriate safeguards.[13]

The second debate on the fight against child sexual abuse is currently still ongoing in the discussions on the proposed (recast) EU Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material.[14] After several years of discussions, EU Member States still have not been able to agree on a common position. In the meantime, as the ePrivacy Directive prohibits chat monitoring, a temporary exception to the confidentiality of communications – which allows providers to voluntarily detect and report sexual abuse of children in their service – has been agreed and extended by August 2026.[15]

Besides, also under the more general updated EU Security Union Strategy (2020)[16], the Commission emphasized that encryption is also used for criminal purposes and promoted "an approach which both maintains the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime and terrorism". In January 2023, Justice and Home Affairs Ministers held an informal meeting to discuss the challenges faced by judicial and law enforcement authorities in accessing data to fight crime in the digital age. Half a year later, in June 2023, the Commission established a High-Level Group on Access to Data for Effective Law Enforcement. This move was intended as a response to the concerns that criminals could exploit encryption and data storage practices to operate in the digital shadow. This group, made up of representatives of Member States, EU agencies, the Commission itself, and the EU Counter-Terrorism Coordinator, made 42 recommendations – from capacity building measures, industry cooperation, and standardisation efforts to new legal frameworks to prevent investigations from "going dark".[17] The group's concluding report describes in detail the challenges identified by the experts and sets out options for operationalising the recommendations.[18]

---

12 For further details, see: Chousou, S./Magaud, J./Pavoni, L/Williams, M. 2023. "Is encryption a fundamental right? A case study on CSAM regulation in the EU". Sciences Po, Section 3, https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/07/Encryption.pdf.

13 European Council conclusions on security and defence, 22/06/2017, para. 2.

14 Proposal COM(2024(60) for a directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA (recast), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52024PC0060 .

15 Regulation (EU) 2024/1307 of the European Parliament and of the Council of 29 April 2024 amending Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse.

16 Communication COM/2020/605 from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, p. 13.

17 Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement.

18 Concluding report of the High-Level Group on access to data for effective law enforcement (15 November 2024).

The Council's formal endorsement of these recommendations in December 2024[19] reflects a broader push to implement concrete measures, including the possibility of reviewing data retention laws and exploring measures that could force service providers to grant access to encrypted communications. At the time, the Hungarian Minister of the Interior, Sándor Pintér, pointed out that: "We cannot allow digitalisation to give a competitive edge to criminals over law enforcement. Access to data is essential so that law enforcement authorities can fulfil their mission of keeping citizens safe."[20] Two particularly controversial measures have emerged at the centre of the debate: (1) the revival or reissue of a mandatory data retention framework (known in Germany as *Vorratsdatenspeicherung*) that has previously been struck down by the EU Court of Justice on proportionality grounds;[21] and (2) the introduction of "backdoors", or special technical measures, that would allow law enforcement agencies to bypass encryption. While officials argue that such tools are needed to fight terrorism, organised crime, and child sexual abuse online, critics warn that these approaches risk undermining the security and privacy of all users, a point to which we return below.

In February 2024, the very idea of reviewing data retention laws and of building up interception capabilities within the EU was addressed by a White Paper of the Commission.[22] It outlined ideas for a so called "Digital Networks Act" (DNA) that is envisaged to be presented by the end of 2025. In particular, the White Paper looked at the issue mostly from an internal markets and competitiveness angle. It claims that there are too many different obligations across the EU with regard to, inter alia, lawful interception and data retention, driven by "cultural and diverging market circumstances" as well as a lack of harmonization of sector rules. Also, it sees deficits in the implementation of EU rules on these topics at national level and criticizes different approaches by Member States with respect to the enforcement of said rules. The divergence of practices, rules, and enforcement habits is seen by the Commission as a barrier for network operators to conduct business across borders within the EU, limiting their growth potential. The discussions raised by the White Paper as well as an accompanying consultation[23] hints towards a willingness on the side of the Commission to achieve a higher consistency and alignment of approaches in the EU in the years ahead.

3 The risks of weakening security

Civil society organisations, digital rights groups, and technology experts have strongly opposed proposals to weaken encryption or impose blanket data retention. In an open letter responding to the High Level Group's recommendations, prominent organisations have now argued that introducing vulnerabilities (such as backdoors in encryption) would create systemic risks affecting millions of users.[24] Encryption, they stress, is not just a tool to enhance privacy – it is essential for securing critical infrastructure, financial transactions, public institutions, as well as the communications of journalists, activists, and human rights defenders.

In our assessment, the argument against backdoors is well-founded. Security experts have long argued that if a vulnerability is created – intentionally or otherwise – it can be exploited not only by law

[19] Council of the EU (2024), Access to data: Council calls for challenges for law enforcement to be addressed - Consilium.
[20] For this quote, see the accompanying Council press release: https://www.consilium.europa.eu/en/press/press-releases/2024/12/12/access-to-data-council-calls-for-challenges-for-law-enforcement-to-be-addressed/.
[21] Jan Podkowik, Robert Rybski, Marek Zubik, Judicial dialogue on data retention laws: A breakthrough for European constitutional courts?, International Journal of Constitutional Law, Volume 19, Issue 5, December 2021, Pages 1597–1631.
[22] European Commission (2024), White Paper - How to master Europe's digital infrastructure needs?.
[23] See: Results of the exploratory consultation on the future of the electronic communications sector and its infrastructure.
[24] See: Open_Letter_on_HLG_Access_to_Data_for_Effective_Law_Enforcement_Recommendations.pdf.

enforcement with a proper warrant, but also by malicious actors, including hostile states or cybercriminals. Technical analyses confirm that such measures cannot be narrowly targeted, creating vulnerabilities exploitable by malicious actors.[25] The unintended consequences could be severe, leading to massive data breaches, undermining trust in digital services, and endangering individuals whose safety depends on secure communications. The European Court of Human Rights (ECtHR) recently ruled that encryption backdoors violate the right to private life under Article 8 of the European Convention on Human Rights.[26]

In contrast, it seems that the EU High Level Group in principle strives for "lawful access" by design to data and intends to avoid solutions that provide for a systematic weakening of encryption.[27] It emphasises that technical solutions must be found which enable targeted, legitimate access to data, admitting that possible new obligations must not lead, directly or indirectly, to obligations for the providers to weaken the cybersecurity of communications for all users of a service by generally undermining or weakening end-to-end-encryption. While the High-Level Group primarily expects service providers to "cooperate" with law enforcement authorities, it states that in case of non-cooperating providers, authorities will still need to resort to the use of vulnerabilities in "exceptional" cases (e.g., primarily criminal services such as EncroChat), and that relevant safeguards and possibly rules for the mutual admissibility of evidence must thus be harmonized.

Critics argue, however, that there is in reality no technical way to break the promise of end-to-end encryption without weakening the security of communications systems, as any backdoor intended for law enforcement can always be – and in various cases has been – exploited by malicious actors.[28] Historical precedents, discussed in Section 4, and the opinions of leading cryptographers confirm that selective weakening of encryption is not technically feasible without compromising the overall security of the system. In this context, it should be noted that the European Data Protection Board (EDPB), the umbrella organisation of European data protection authorities, emphasised in November 2024 that technical measures that could weaken encryption are not limited to introducing a "backdoor" into the encryption process itself.[29] Rather, also the introduction of a client-side process allowing remote access to data before its encryption or after its decryption at the recipient would – though not technically weakening encryption – likely lead to substantial, untargeted access and thus undermine the security and confidentiality of their communications.

A game-theoretical lens helps to illuminate our reasoning about the systemic risks inherent in backdoor mandates. By forcing a regulatory intervention that treats all users as potential surveillance targets, authorities effectively collapse the cryptographic ecosystem into a *pooling equilibrium*, i.e. a scenario where platforms cannot distinguish between lawful users and malicious actors through technological design; in contrast to the *separating equilibrium* solution, where only vetted entities use strong encryption. This creates perverse incentives: hostile states and cybercriminals gain asymmetric advantages from the universal security degradation, while ordinary users and businesses bear the costs

[25] See: Computer Science and Artificial Intelligence Laboratory (2025), Technical Report "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications", MIT-CSAIL-TR-2015-026.pdf; IAB Statement on Internet Confidentiality; End-to-End Encryption and the Web.

[26] Perez (2024), The European Court of Human Rights Concludes Encryption Backdoor Mandates Violate the Right to Private Life of All Users Online - Center for Democracy and Technology.

[27] Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement.

[28] See: Open_Letter_on_HLG_Access_to_Data_for_Effective_Law_Enforcement_Recommendations.pdf.

[29] EDPB (2024), Statement 5/2024 on the Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement | European Data Protection Board.

of weakened protections. These vulnerabilities effectively transform encryption from what we could regard as a *public good* (secure communication that benefits everyone) into its opposite: once a backdoor is imposed, malicious actors' exploitation of that weakness harms all users. As this harm is non-excludable (no one can easily opt out of the forced vulnerability), this makes it akin to a *public bad*.[30] Indeed, this equilibrium shift would likely manifest in measurable economic harm, as 62% of small and medium-sized entities (SMEs) anticipate reduced hiring and 58% plan investment cuts under backdoor regimes.[31] In other words, security dilution alters market calculations – not through direct hacking costs, but through eroded trust in digital infrastructure. The Stackelberg dynamics[32] between regulators (as first-movers, or leaders, imposing security constraints) and attackers (as followers, exploiting newly created vulnerabilities) create a negative-sum game: every percentage point gain in law enforcement access capacity could enable exponentially larger attack surfaces for bad actors.

While game theory thus suggests that blanket security reductions create negative-sum outcomes, the EU's recent debates, which we surveyed in Section 2 above, suggest that some policymakers might accept this sub-optimal equilibrium as an unavoidable *trade-off for strategic autonomy*. Tightening regulatory reins might offer governments more direct influence in compelling foreign providers to comply with domestic laws, thereby reinforcing a sense of control over data flows and digital infrastructure. Indeed, proposed regulatory interventions typically extend beyond weakening encryption to encompass data localization requirements, ex-ante platform approvals, and asymmetric compliance burdens on foreign firms. In the context of the forthcoming EU internal security strategy, the issue of encryption could thus be included in this broader debate and framed as a strategic choice: accepting some vulnerability for citizens in exchange for better oversight. In our assessment, however, the ultimate price may be too high: undermined user trust, weakened cybersecurity, and the chilling effect on innovation and SME investment. Moreover, the ECtHR's admonition on backdoors shows that there are also clear legal risks. If EU policymakers are nevertheless inclined to force this trade-off, they must recognize that the costs of weakened encryption, borne primarily by users (both domestic and foreign), are neither trivial nor easily reversible, and could well ripple through the entire digital ecosystem.

Equally controversial as weakening encryption is the push for broad, indiscriminate data retention measures. Proponents argue that if the threat changes, the proportionality of countermeasures must change accordingly, and that therefore the compulsory retention of IP addresses would be compatible with Union law.[33] However, previous attempts at mandatory data retention legislation at EU level have run afoul of the EU Charter of Fundamental Rights, leading courts to emphasise the need for strictly proportionate, targeted, and time-limited measures. A potential alternative to blanket retention would be the "quick freeze" procedure, which is also popular in the German debate. Unlike broad, indiscriminate data retention – which stores bulk communication metadata (e.g., location data, call logs) and IP addresses for entire populations – quick freeze allows authorities to preserve specific data only when there is prior judicial authorization tied to a concrete suspicion of serious crime or national security threats.[34] In essence, quick freeze represents a more rights-respecting alternative to blanket retention, prioritising judicial oversight and specificity. However, its efficacy depends on timely investigations and provider compliance.

---

30 For this distinction, see: Buchholz, Cornes, Rübbelke (2017), Public Goods and Public Bads, CESifo Working Paper No. 6437.
31 This data comes from: Gladwin et al. (2024), Backdoors and Balance Sheets, p. 3.
32 For an example of how to model such a Stackelberg game in the context of cyberthreats, see: Yang and Zhu (2024), Game-Theoretic Foundations for Cyber Resilience Against Deceptive Information Attacks in Intelligent Transportation Systems.
33 Herrmann (2024), More Protection for Victims Through Data Retention.
34 Bertuzzi (2022), Europe seeks a way out of the data retention pickle | IAPP.

4 Lessons from across the Atlantic?

A recent episode from the US provides an illustrative cautionary tale. For decades, some US law enforcement and intelligence agencies advocated "exceptional access" to encrypted communications, claiming that only criminals needed such robust privacy protections – echoing the current debate in the EU. But over the past months, a dramatic shift occurred following revelations that Chinese state-sponsored hackers had infiltrated major US telecommunications networks, gaining access to call metadata and possibly even live calls (the so-called "Salt Typhoon" hack). Specifically, the Chinese hackers exploited systems that US telecom companies had built to comply with federal wiretapping laws such as Communications Assistance for Law Enforcement Act (CALEA), which requires telecommunications firms to enable "lawful intercepts". In theory, these built-in channels were supposed to only give law enforcement an exclusive window into suspect communications. In practice, however, they became a universal vulnerability that hostile actors could just as easily exploit. Suddenly, the very government voices that once dismissed end-to-end encryption began recommending that citizens use encrypted messaging apps to maintain their security.[35]

What can we learn from this? While governments often push for greater surveillance capabilities, the real and current threat of state-sponsored cyber-espionage demonstrates the indispensable value of strong encryption. As the Electronic Frontier Foundation has noted, Salt Typhoon shows once more that there is no such thing as a backdoor that only the "good guys" can use.[36] If the mechanism exists, a malicious party will eventually find it and weaponise it. The lesson for Europe is clear: undermining encryption to aid investigations may prove short-sighted if it also exposes citizens – and state institutions – to hostile foreign interference. Is this really what we want to do in an increasingly challenging geopolitical environment? The debate about ensuring lawful and effective access to data in the digital age will remain one of the most pressing challenges, so we need to ask whether there are alternative, viable models.

5 Are there alternative models?

EU policymakers must find a way to provide law enforcement with the tools they need to fight crime, while preserving the fundamental rights that underpin the EU's political and legal order. This is another example of the many dilemmas that currently permeate EU digital policymaking.[37] According to a joint statement, European police chiefs do not accept that there has to be a binary choice between cybersecurity or privacy on the one hand and public safety on the other, arguing that technical solutions exist but require flexibility from industry and governments alike.[38]

Indeed, from a law enforcement perspective, encrypted chats are just one small piece of a much larger digital information space. While law enforcement authorities increasingly demand access to encrypted data, representatives of encrypted messaging services argue that there are other ways for law enforcement to investigate crimes without having to break into encryption, which include monitoring unencrypted chats, social media, and analysing metadata from communications.[39] As Canadian experts have noted in 2021: "There is a plethora of non-encrypted data available to police and security agencies to

---

35 Collier (2024), U.S. officials urge Americans to use encrypted apps amid cyberattack.
36 Mullin and Cohn (2024), Salt Typhoon Hack Shows There's No Security Backdoor That's Only For The "Good Guys", EFF.
37 Küsters and Sottilotta (2025), Trade-Offs and Risks in EU Digital Policy | cep - Centre for European Policy Network.
38 See: EDOC-#1384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF.
39 Goodwin (2025), Europol seeks evidence of encryption on crime enforcement as it steps-up pressure on Big Tech | Computer Weekly.

lawfully gather and analyze for investigative and intelligence gathering purposes, including open source data (e.g., social media and other online data). Such approaches need to be guided by best practices, given their criticisms and broader worry surrounding their use."[40]

For example, criminals leave digital footprints almost everywhere they go, from credit card transactions, location data from apps, social media posts, GPS trackers, and more. According to an Associated Press investigation, an obscure tool called "Fog Reveal" has allowed US police to track people's movements for months using cellphone signals, all at relatively low cost and often without a warrant.[41] Critics call it "mass surveillance program on a budget", as it can reconstruct "patterns of life" from people's daily activities. Be that as it may, with such powerful investigative techniques already in play, agencies do not need to blow end-to-end encryption for everyone just to catch a handful of criminals. From this perspective, policymakers should instead focus on more discriminating tactics that use existing tools (such as Fog Reveal) in a transparent, legally accountable way, rather than tearing a hole in the security fabric on which modern digital life depends. But is this sufficient?

Obviously, simplistic or dangerous solutions should be avoided. Likewise, as the EDPB has rightly pointed out, the EU should not set up contradictory demands for providers to both allow for the interception of specific communications and not indiscriminately weaken encryption, obliging them to find the means to comply.[42] This would lead to strong uncertainty for the providers, possible incoherent enforcement and ultimately undermine the finding of the right balance. The High-Level Group has recommended to establish a research group to assess the technical feasibility of built-in lawful access obligations (including for accessing encrypted data) for digital devices, without compromising the security of devices or communications. It is currently unclear whether standards for present and future communication technologies can be developed which enable lawful access without weakening privacy, as proposed by the experts.

As regards data retention, rapid freezing procedures as well as transparent and judicial safeguards could provide practical alternatives to mass surveillance. However, it is important to acknowledge that these freezing procedures have faced criticism themselves, e.g. for potentially being insufficient or implemented too late.[43] Critics argue that by the time a freezing order is issued, relevant data may no longer be available, as providers often store IP addresses for only short periods, ranging from a few hours to several days. This limitation could significantly impair the effectiveness of quick freeze methods in combating serious crimes, particularly in cases of child sexual abuse where timely access to data is crucial. Despite these concerns, proponents argue that freezing procedures still offer a more targeted approach compared to indiscriminate mass data retention. In the face of this epistemological and technical uncertainty, trust should remain at the heart of Europe's digital future and not be jeopardised by overtly aggressive law enforcement reforms.

---

[40] Masoodi and Rand (2021), Why Canada Must Defend Encryption, https://www.cybersecurepolicy.ca/policy-brief-encryption, p. 4.

[41] See: PBS (2022), How an obscure cellphone tracking tool provides police 'mass surveillance on a budget'.

[42] EDPB (2024), Statement 5/2024 on the Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement | European Data Protection Board.

[43] For the debate, see: Krempl (2024), Quick Freeze: Activists warn against data retention through the back door, Heise; Herrmann (2024), More Protection for Victims Through Data Retention; and EDRi (2020), Data Retention Revisited.

We conclude this section with a brief outlook on quantum computing, which will add to this uncertainty. While predictions about the speed of this transformation vary widely,[44] it seems safe to say that the advent of quantum computing will introduce a new phase shift in the regulatory calculus, forcing policymakers to reevaluate the cryptography-law enforcement equilibrium discussed in this cepAdhoc. While current debates focus on preserving classical encryption, quantum capabilities could render these protections obsolete within a decade, as NIST-approved post-quantum cryptography (PQC) standards suggest existing (asymmetric) encryption will collapse.[45] In the context of our argument, it is important to point out that quantum computing does not resolve the encryption-access dilemma. The ECtHR's Article 8 protections would face novel challenges from quantum decryption of historical communications, potentially requiring jurisprudence to define temporal limits on cryptographic obsolescence. To counter the systemic risks from this transformation, experts argue that firms should adopt PQC as a precautionary measure,[46] a principle enshrined in Art. 191(2) of the Treaty on the Functioning of the EU. The future regulatory situation hinges on whether quantum becomes, in the sense of our game-theoretical framework introduced above, a separating equilibrium tool or not: If the EU maintains quantum decryption capabilities as state-exclusive resources (e.g. via its forthcoming quantum strategy), it could theoretically preserve encryption integrity for civilians while reserving quantum brute-force attacks for warranted investigations. But such a scenario seems unlikely, given the progress made in other regions of the world and the high economic stakes of quantum technology. In other words, quantum advances are likely to proliferate too quickly for traditional non-proliferation frameworks. Ultimately, therefore, our best guess is that quantum computing will lead to a dynamic arms race that will require regulatory agility that current digital policy structures often lack.

6 Conclusion and outlook

Europe is at a critical juncture in the debate on enhanced data storage and data access for law enforcement purposes. The EU's plans come at a time characterised by abrupt changes in the geopolitical situation and recurring uncertainty regarding existing legal frameworks for transatlantic data transfers and data access. The EU is facing a huge and extremely complex balancing act in order to reconcile common security needs, diverging national security interests of its Member States, and the fundamental rights of its citizens. Due to the potential risks and the "sensitivity of public debate", law enforcement experts have suggested a gradual and evidence-based approach involving all relevant experts.[47] Presumably to pursue this approach, the European Commission and Europol are, according to media reports, trying to gather evidence to show how encryption technologies are counteracting criminal investigations.[48] It is, however, not clear whether these examples will be released publicly.

The Council has mandated the European Commission to prepare a roadmap by the end of June 2025 for the implementation of concrete measures to guarantee access to data for effective law enforcement, taking into account the relevant case law of the Court of Justice of the EU and with full respect

[44] According to Moody, "implementing new cryptographic standards across devices could take 10 to 15 years due to operational challenges, though swift deployment by some tech companies will accelerate protection for many users". See: https://industrialcyber.co/reports/moodys-sounds-alarm-on-quantum-computing-risk-as-transition-to-pqc-will-be-long-and-costly/.

[45] See: https://vivatechnology.com/news/quantum-s-impact-on-cybersecurity.

[46] Jančiūtė (2025), Cybersecurity in the financial sector and the quantum-safe cryptography transition: in search of a precautionary approach in the EU Digital Operational Resilience Act framework, Int. Cybersecur. Law Rev.

[47] Concluding report of the High-Level Group on access to data for effective law enforcement (15 November 2024).

[48] Goodwin (2025), Europol seeks evidence of encryption on crime enforcement as it steps-up pressure on Big Tech | Computer Weekly.

for fundamental rights. This roadmap shall contain for each measure a precise timetable and the proposed way of implementing them, including an analysis of the appropriate resources needed. It is expected that the Commission will likely push for more harmonization what data service providers must retain and how law enforcement agencies can access it.[49] The Internal Security Strategy due to be presented on 1 April, and the Digital Networks Act (DNA) envisaged for the end of the year, will hopefully provide welcome detail and clarification on the EU's vision in this field for the years ahead.

At first glance, it appears positive that both the High-level group[50] and the Council[51] seem to be looking for a collaborative solution between law enforcement and service providers. However, law enforcement should not from the outset be built on the forced "collaboration" of telecommunications and OTT service providers with law enforcement agencies. Instead, despite and precisely because of the sensitivity of the public debate and given the technical complexity and political uncertainties, an open public discourse with active and constructive contribution not only of the Commission and the Member States and their law enforcement agencies, but also of the service providers and all relevant stakeholders seems to be unavoidable as a starting point for finding an appropriate, acceptable, and fundamental rights-compliant solution. Aggressive measures like encryption backdoors or bulk data retention lack evidence of efficacy but carry demonstrable risks such as undermining cybersecurity and eroding citizen confidence in institutions. Policymakers must instead anchor reforms in proportionality and rights-respecting tools such as targeted "quick freeze" to safeguard democratic values.

More broadly, the shift from an analogue to a digital world has profoundly altered the interplay between individuals, markets, and governments by magnifying the role of data and making national borders more porous. Where state power once extended through physical searches or phone taps, it now encounters encryption, digital networks, and powerful platform providers.[52] As just one example of many, consider how Telegram handed over more user data to French authorities after Pavel Durov, the messaging app's founder and CEO, was arrested in Paris last August over criminal content posted by users on his platform.[53] A coherent view of regulatory or ordering policy (*Ordnungspolitik*) requires balancing the qualitatively new challenges to public security with an unwavering commitment to democratic principles, while recognising the inherent transnational dimension of modern technology. Our discussion of encryption shows that the answers to this trilemma are not always straightforward and can often backfire, for example, when sweeping regulatory interventions threaten to undermine both civil liberties and the very security they are intended to enhance. Even more than previously, therefore, policymakers should seek evidence-based, proportionate, and collaborative frameworks for "ordering" the digital. Our lessons learned from the current encryption debates thus point to the broader challenge of transitioning to a model of governance that effectively addresses the complexities of the digital world without compromising fundamental freedoms or undermining the core values of the European project.

---

[49] See: Corca and Echarren (2025), EU Policy & Regulatory | Law Enforcement Access to Data: A (re)newed Chapter in EU Digital Policy | Considerati.

[50] Concluding report of the High-Level Group on access to data for effective law enforcement (15 November 2024).

[51] See: Council conclusions on access to data for effective law enforcement – Council conclusions (12 December 2024), pdf.

[52] Lehdonvirta (2022), Cloud Empires. How Digital Platforms are Overtaking the State and how we can Regain Control, MIT Press.

[53] See: https://www.lemonde.fr/en/pixels/article/2025/01/08/telegram-gave-more-user-data-to-french-authorities-after-founder-s-arrest_6736824_13.html.

Centrum für Europäische Politik
FREIBURG | BERLIN

Authors:

Dr. Anja Hoffmann, LL.M. Eur.
Policy Analyst
Single Market and Competition Policy | Digital Economy
hoffmann@cep.eu

Dr. Anselm Küsters, LL.M. Eur.
Head of Department
Digitalisation and New Technologies
kuesters@cep.eu

Philipp Eckhardt
Head of Department
Financial Markets and Information Technologies
eckhardt@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Raum 4205 | D-10117 Berlin
Tel. + 49 761 38693-0

The **Centrum für Europäische Politik** FREIBURG | BERLIN, the **Centre de Politique Européenne** PARIS, and the **Centro Politiche Europee** ROMA form the **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

Free of vested interests and party-politically neutral, the Centres for European Policy Network provides analysis and evaluation of European Union policy, aimed at supporting European integration and upholding the principles of a free-market economic system.