European Union's looming attack on encryption

State of play

26 June 2026

Chloé Berthélémy, Senior Policy Advisor, European Digital Rights

EDRi

Content

01 Current and historical context

02 Encryption under attack in mandate 2024-2029

03 Expert Group for a Technology Roadmap - first meetings

EDRi

Increasing pressure at national level

Swedish authorities seek backdoor to encrypted messaging apps

Sweden's law enforcement and security agencies are pushing legislation to force Signal and WhatsApp to create technical backdoors allowing them to access communications sent over the encrypted messaging apps.

France pushes for law enforcement access to Signal, WhatsApp and encrypted email

Proposals to be discussed in the French Parliament will require tech companies to hand over decrypted messages and email or face huge fines



By **Bill Goodwin,** Investigations Editor

Published: **28 Feb 2025 16:56**

The Washington Post
Democracy Dies in Darkness

Tech Help Desk Artificial Intelligence Internet Culture Space Tech Policy

EXCLUSIVE

U.K. orders Apple to let it spy on users' encrypted accounts

Secret order requires blanket access to protected cloud backups around the world, which if implemented would undermine Apple's privacy pledge to its users.

Updated February 7, 2025 More than **1 year ago**

Danish Justice Minister Under Fire for Pushing Encryption Ban While Using It

Denmark's push to block encrypted apps fuels debate over privacy vs. surveillance, with critics calling out the hypocrisy of those in power.



by **Didi Rankovic** August 31, 2024 2 min read + subscribe ↗ share

EDRi

Constant tension

EU in the post-Snowden era Crypto War

- 2017 Security Union report: “encryption is essential to ensure cybersecurity and the protection of personal data”
- But also “major threat to the detection, investigation, and prosecution of crimes”
- Council resolution, 2020 “Security through encryption, security despite encryption”

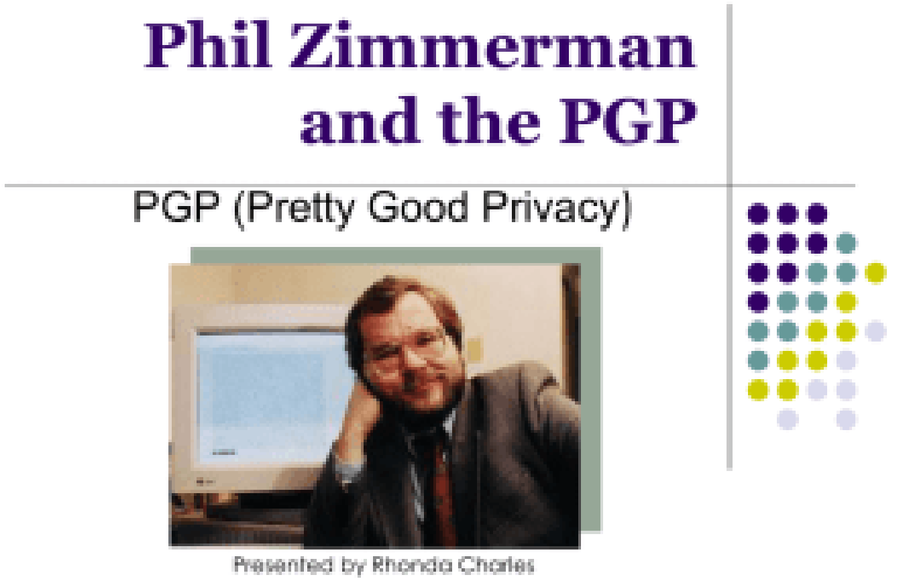
*“strike the **right balance** between ensuring the continued use of strong encryption technology and **guaranteeing the powers of law enforcement** and the judiciary to **operate on the same terms as in the offline world**.”*



Old history

The crypto wars are many





EDRi

2010s



2009



2010



2010



2012



2013

EDRi

2010s



WIRED SECURITY POLITICS THE BIG STORY BUSINESS SCIENCE CULTURE REVIEWS

The FBI Wanted a Back Door to the iPhone. Tim Cook Said No

The agency wanted to crack the iPhone of Syed Farook, a suspect in the 2015 San Bernardino shooting. The Apple CEO took a stand.



CASEY CHIN: GETTY IMAGES

EDRi

2020s

International Statement: End-To-End Encryption and Public Safety

Sunday, October 11, 2020

For Immediate Release

Office of Public Affairs

We, the undersigned, support strong encryption, which plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security. It also serves a vital purpose in repressive states to protect journalists, human rights defenders and other vulnerable people, as stated in the 2017 resolution of the UN Human Rights Council[1]. Encryption is an existential anchor of trust in the digital world and we do not support counter-productive and dangerous approaches that would materially weaken or limit security systems.

Particular implementations of encryption technology, however, pose significant challenges to public safety, including to highly vulnerable members of our societies like sexually exploited children. We urge industry to address our serious concerns where encryption is applied in a way that wholly precludes any legal access to content. We call on technology companies to work with governments to take the following steps, focused on reasonable, technically feasible solutions:

- Embed the safety of the public in system designs, thereby enabling companies to act against illegal content and activity effectively with no reduction to safety, and facilitating the investigation and prosecution of offences and safeguarding the vulnerable;
- Enable law enforcement access to content in a readable and usable format where an authorisation is lawfully issued, is necessary and proportionate, and is subject to strong safeguards and oversight; and
- Engage in consultation with governments and other stakeholders to facilitate legal access in a way that is substantive and genuinely influences design decisions.

IMPACT ON PUBLIC SAFETY

Law enforcement has a responsibility to protect citizens by investigating and prosecuting crime and safeguarding the vulnerable. Technology companies also have responsibilities and put in place terms of service for their users that provide them authority to act to protect the public. End-to-end encryption that precludes lawful access to the content of communications in any circumstances directly impacts these responsibilities, creating severe risks to public safety in two ways:

EDRi

2020s

Meta encryption plan will let child abusers ‘hide in the dark’, says UK campaign

In Home Office initiative, survivors urge Mark Zuckerberg to rethink changes to Messenger and Instagram



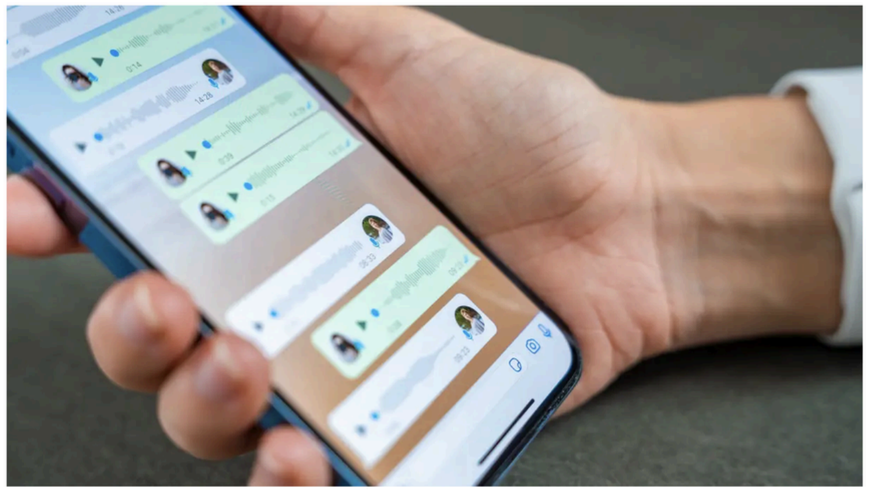
Mark Zuckerberg, CEO of Meta, on Capitol Hill. Photograph: Nathan Howard/Getty Images

heise online heise+ entdecken

heise+ Newsticker Security IT & Tech Developer KI Entertainment Wissenschaft B

EU backs away from chat control

In its new draft for combating child abuse online, the EU is abandoning chat control. Instead: risk assessments and voluntary measures.



EDRi

Updates chat control

CSAR + Provisional ePrivacy Directive derogation

- Derogation to ePD allows communications providers to derogate from privacy protections and do **voluntary detection** of text and images/videos:
  - Extended several times, until April 2026
  - European Parliament rejected the new extension
  - Now, Council wants to send the text to second reading and force the EP to vote again

- CSAR covers the mandatory scanning of communications:
  - A lot is still undecided: scope of content, type of communication, age verification, targeted vs mass, etc.
  - Encryption *a priori* protected
  - Attempt to finalise the trilogues next Monday (29/06)

EDRi

2020s

Operation SKY ECC

- **Target:** Drugs, Money laundering, Corruption, Child sexual abuse material
- **Coordination:** Europol
- **Partners:** Belgium, France, Netherlands
- **Participating agencies:** EUIPO, Eurojust, Frontex, INTERPOL, OLAF, WADA
- **Duration:** March 2021 – ongoing

NEWS

International operation takes down another encrypted messaging service used by criminals

It is not the first time and will not be the last time that authorities are able to read criminals' messages in real time

Home / Media & press

NEWS

Global Coalition Takes Down New Criminal Communication Platform





EDRi

Law enforcement’s strategy

Undermining the reputation of encryption

SkyECC/EncroChat operations

- Bulk hacking operations in 2019-2022: ‘successful’ at circumventing encryption but raise many legal and political issues.

- Operations’ goals:
  - delegitimising encrypted apps: instilling a presumption of criminality
  - pushing for the principle that no communication or data must be beyond the effective reach of law enforcement or intelligence services
  - showcasing the need for a legal solution aka mandated backdoors

Law enforcement’s strategy

Undermining the reputation of encryption

“Criminal investigations now contain an element of chance — something that is unacceptable for law enforcement, for victims and for society as a whole”

Catherine De Bolle, Executive director of Europol
Cyrus R. Vance, Jr., District Attorney of New York County


NEWS › OPINION

The last refuge of the criminal: Encrypted smartphones

Encryption unregulated is justice denied.

SHARE

Technology is moving quickly, and the criminal abuse of it is no exception | Gabriel Bouys/AFP via Getty Images

OPINION

JULY 26, 2021 4:01 AM CET

Law enforcement’s strategy

Undermining the reputation of encryption

Push for backdoors

- Joint Declaration of the European Police Chiefs, April 2024
- Europol, First report on encryption, June 2024
- Eurojust & Europol, Common challenges in cybercrime, 2024





Encryption in mandate 2024-2029

High Level Group “Access to Data for Effective Law Enforcement” or “Going Dark”

- Working group set up by the Commission in **June 2023**;
- Co-chaired by the EU Commission and the rotating EU Council Presidency;
- Composed of **EU MS “experts”** (mainly from prosecution offices, law enforcement authorities), few observers from a data protection perspective;
- Not a typical “high-level expert group” = **opaque process**;
- **Mission**: officially, the group is tasked with listing “recommendations for the **further development of Union policies** to enhance and improve access to data for the purpose of effective law enforcement.”

EDRi

42 Recommendations - 4 main concerns

Encryption backdoors and data retention

Obligation to build in backdoors/vulnerabilities, called “lawful access by design”
Obligation to decrypt
Obligation to collect and retain

Real-time interception

Rules for cross-border real-time interception (data in transit)

Harsh sanctions for non-compliance

Fines, market ban, individual liability

Scope

All “data handlers” (telecoms, email providers, social media, messaging services, smart and connected objects, etc.) + hardware manufacturers

Encryption in mandate 2024-2029

ProtectEU Internal Security Strategy, 1 April 2025

The Commission will:

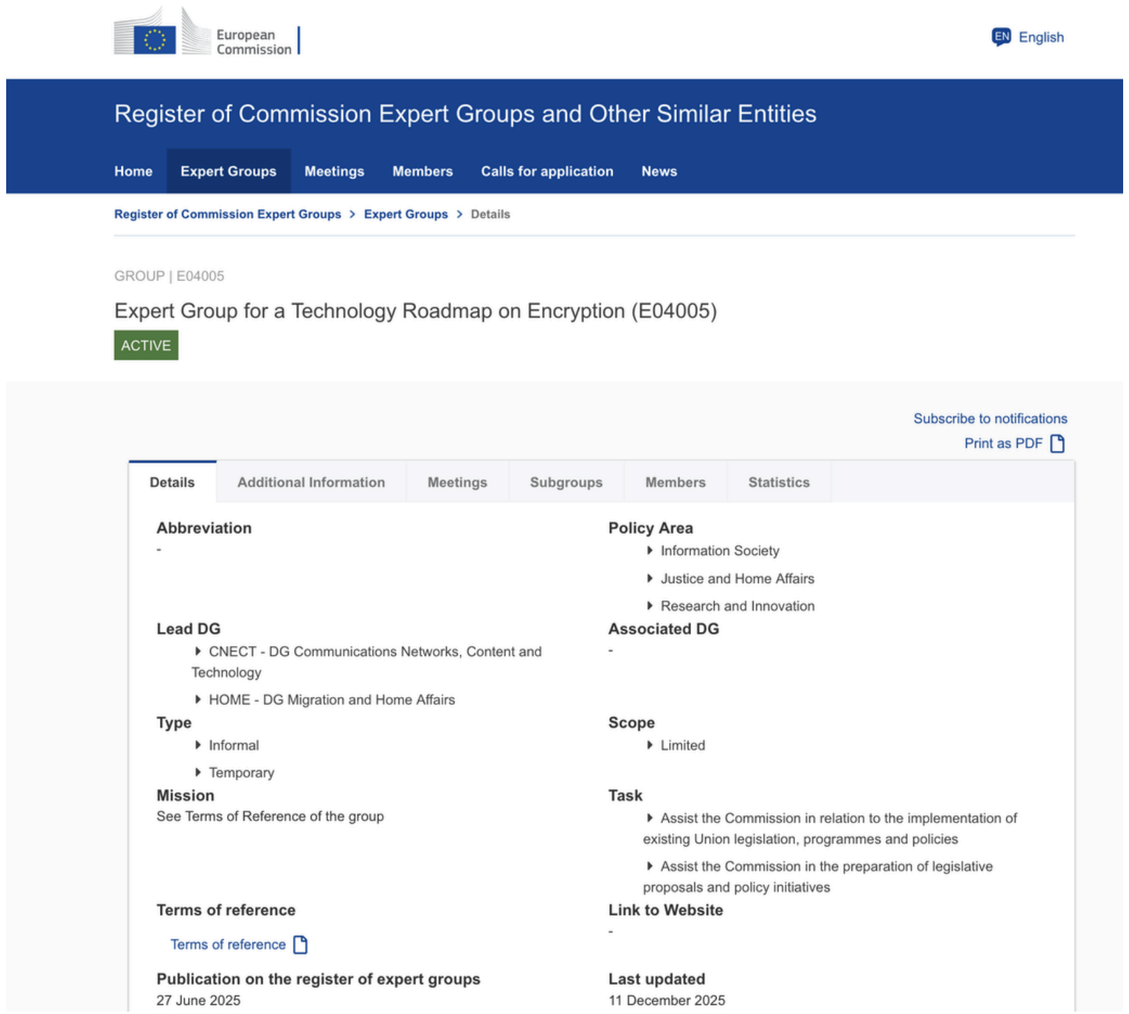
- **present a Roadmap setting out the way forward on lawful and effective access to data for law enforcement in 2025**
- **prepare an impact assessment in 2025 with a view to updating rules on data retention at EU level, as appropriate**
- **present a Technology Roadmap on encryption to identify and assess technological solutions to enable lawful access to data by law enforcement authorities in 2026**
- **work towards creating a High-Level Group to strengthen operational law enforcement cooperation**
- **create a Security Research & Innovation Campus at its Joint Research Centre in 2026**

EDRi



EDRi

Expert Group for a Technology Roadmap



EDRi

Terms of Reference

"The work should notably focus on **fixed and mobile communications and devices**, where lawful access to data is impacted by. It should also address encryption in the **context of digital forensics** and **of data retention**.

The group should identify **potential technical options** and **assess their suitability** to improve lawful access to data by law enforcement, [focusing] on technologies that are **already available or possibly developed in the future** (…)

(…) the technology roadmap should **examine the risks** these technologies present, including risks posed by sophisticated nation state threat actors and technical, behavioural, and organisational risk factors [and] consider technical and organisational measures to **address, mitigate and possibly remedy such risks**"

EDRi

Criteria for assessment of possible solutions

Feasibility and operational efficacy

- Serve law enforcement's objectives?
- Cross-border orders and multiple access requests
- Scalability
- Easiness for targets to avoid access
- No detection
- Performance if targets are switching network connections
- Costs
- Timeframe
- Service Providers involvement

Cybersecurity and robustness

- Robustness against misuse by nation state actors and other malicious actors ?
- Increases of the attack surface?
- Impacts on the level of cybersecurity
- Impacts on use of cybersecurity best practices, standards and techniques?
- Use of weaker protocols?
- Impact of accidental disclosure of a single key on large number of devices
- Service Providers' trustworthiness
- Sovereignty, existing legislation and jurisdiction

Criteria for assessment of possible solutions

Targeted approach, privacy and data protection

- Indiscriminate monitoring
- Infringement on the privacy of communications and data of other individuals not subject to the lawful access process
- Data collected protected from unauthorised access

Transparency and auditability

- Demonstrating legality of access
- Oversight and checks
- Enabling targets to seek and benefit from legal remedies
- Keeping track of its usage

Necessity, preventing abuse and proportionality

- Ensure proportionality of its use
- Limitations of rights and freedoms
- Avoid abuse and single point of failure internal to the service provider or law enforcement authority,
- Indications of abuse can be reported to relevant authorities
- Respect of a time-boxed warrant (only data posterior to the set-up of the measure can be accessed)

Mapping solutions

Data at rest in law enforcement's possession

- Seized devices or cloud-stored data where keys may reside with service providers
- Software-based and hardware-backed
- Weakening encryption explicitly rejected
- Options:
  - Manufacturer cooperation (detailed product documentation)
  - Cloud-based key escrow (storing device-specific recovery keys)
- Transparency mechanisms

Real-time access to encrypted communications in transit

- Server interception
- Client-side scanning out of scope
- Key escrow only to targeted communications
- End-to-End Encryption (E2EE): necessary safeguards to "accompany any potential adaptation of the encryption protocols"
- Common reference architecture to define interfaces and functionalities for lawful interception systems

Mapping solutions

Targeted remote access techniques (**covert techniques**)

- Pushing modified app versions to suspects' devices via communication providers
- Monitoring agents: "A semantic and legal distinction was drawn between lawfully authorised monitoring tools and illegal spyware, though technical and ethical hurdles remain"

- No minutes for April meeting
- No agenda for June meeting available yet?
- Expected final outcome: Early 2027

QUESTIONS?