Scanning private communications in the EU

EDRi's principles for derogating from the ePrivacy Directive for the purpose of detecting online child sexual abuse material (CSAM)

9 February 2022

With many thanks to members of the EDRi network for their work on this paper, in particular Bits of Freedom, Dataskydd.net, Digitalcourage, Digitale Gesellschaft, the Foundation for Information Policy Research, the IT-Political Association of Denmark and Privacy International.

Executive summary

The automated scanning of everyone's private communications, all of the time, constitutes a disproportionate interference with the very essence of the fundamental right to privacy. It can constitute a form of undemocratic mass surveillance, and can have severe and unjustified repercussions on many other fundamental rights and freedoms, too.

EDRi's goal is to make sure that any EU proposal to detect online child sexual abuse material (CSAM) is in line with the EU's fundamental rights obligations, **in particular that measures are lawful and objectively necessary and proportionate to their stated goal**. The surveillance or interception of private communications or their metadata for detecting, investigating or prosecuting online CSAM must therefore be limited only to genuine suspects against whom there is reasonable suspicion, must be duly justified and specifically warranted, and must follow national and EU rules on policing, due process, good administration and fundamental rights safeguards. **We propose 10 indivisible principles to ensure that vital efforts to investigate and prosecute those who spread CSAM can be undertaken in a way that is democratic, compatible with European values, and therefore the most likely to achieve justice for victims. This includes Member States taking action on the numerous existing recommendations to address CSAM.**

Policy background

In July 2021, the Council of the European Union reached an agreement with the European Parliament to pass a new law, creating a temporary exception (derogation) from certain parts of the 2002 ePrivacy Directive.

The ePrivacy Directive (2002) is the EU's only instrument containing specific protections for everyone's right to a private life and confidentiality of communications, as enshrined in Article 7 of the Charter of Fundamental Rights of the EU (CFREU). In 2018, the recast of the European Electronic Communications Code (EECC) expanded the definition of an 'electronic communications service'. This expansion meant that since December 2020, certain rules in the ePrivacy Directive now apply to a wider range of online services.

This was the catalyst for the European Commission to put forward the temporary derogation from the ePrivacy Directive, in order to legalise the ongoing voluntary scanning of private communications by service providers. The derogation will expire in August 2024, and the European Commission intends to replace it with a long-term law (expected March 2022).

Discussion of relevant EU and international law

The right to the privacy of communications (Article 7, CFREU) ensures that everyone can seek out health and legal advice, confide in friends and family, and build support networks online without undue interference. It protects the messages of journalists and human rights defenders, safeguarding the sources on whom they rely to expose corruption and organise for social change. In these ways and more, privacy is a foundation for enjoying almost all other fundamental rights. As asserted by the United Nations (UN) High Commissioner on Human Rights, Michelle Bachelet:[1]

> *"the right to privacy plays a pivotal role in the balance of power between the State and the individual and is a foundational right for a democratic society."*

That is why any limitation on the right to privacy must be based on law, serve a legitimate aim in a democratic society, and be necessary and proportionate to that aim.

Children's privacy:

The right to privacy is perhaps even more important for young people, given the profound impact that violations can have on their self-development. As the UN recognises in its 2021 'General Comment No. 25 on children's rights in relation to the digital environment', developed in consultation with 709 young people, "[p]rivacy is vital to children's agency, dignity and safety and for the exercise of their rights" (¶67).[2] UNICEF's 2018 toolkit on children's online privacy adds:[3]

1 https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E
2 https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf, page 8
3 https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

"Children's communications privacy is threatened where their posts, chats, messages or calls are intercepted by governments or other actors".

UN General Comment No. 25 also makes several recommendations about children's privacy which are highly relevant to the scanning of private online communications:

- "**Any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately** or without the child's knowledge [...] ; **nor should it take place without the right to object to such surveillance**, in commercial settings and educational and care settings, and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose." (¶75);

- "Technologies that monitor online activities for safety purposes, such as tracking devices and services, if not implemented carefully, may prevent a child from accessing a helpline or searching for sensitive information." (¶76);

- "Protecting a child's privacy in the digital environment may be vital in circumstances where parents or caregivers themselves pose a threat to the child's safety or where they are in conflict over the child's care." (¶77).

Court of Justice of the European Union (CJEU):

Several cases at the CJEU have confirmed that the generalised access to the content of electronic communications by public authorities violates the essence of the right to privacy. See, for example, judgements in cases by *Digital Rights Ireland Ltd* (C-293/12) (2014) and *Maximilian Schrems* (C-362/1) (2015). This will be explored in more detail in our upcoming paper on the proposed long-term derogation.

The General Data Protection Regulation (GDPR):

Privacy by design and default means that we should all be able to fully enjoy our right to privacy, up to and until the point when there is a legitimate reason for this right to be limited. However, the automated scanning of everyone's private communications turns this principle on its head. It treats each and every one of us as if we are suspected of looking at or disseminating CSAM online, and spies on us on this basis.

It is also important to note that the temporary ePrivacy derogation (2021) does not provide a legal basis, even for the *voluntary* scanning of private communications. This means that, whilst the derogation exempts these scanning practices from the rules of the ePrivacy Directive, the General Data Protection Regulation (GDPR) still applies. The European Parliament have noted that such scanning practices may be unlawful under the GDPR.[4]

4 https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-temporary-derogation-from-the-e-privacy-directive-for-ott-services

The 10 Principles

Measures to detect, investigate or prosecute online CSAM must always be compliant with national and EU-wide obligations to fundamental rights. At a minimum, we believe that all 10 of the following principles must be met cumulatively, in order **to ensure that the principles of necessity and proportionality are objectively met in upcoming CSAM legislation**:

1. **No mass surveillance**: the generalised, automated scanning of everyone's private communications, all of the time, is a fundamentally disproportionate interference with the right to privacy. Whether for detecting CSAM or for other purposes, such practices are never justifiable in a democratic society. Accordingly, service providers must not be mandated to conduct the generalised automated scanning of private communications;

2. **Interventions must be targeted on the basis of individual-level suspicion**: any interception of private communications must target only the person or persons under investigation (not other users of the service), based on specific, reasonable, individual-level suspicion (e.g. the surveillance of all users of a particular service cannot be considered targeted). The singling out of a suspect is what justifies their surveillance; singling them out cannot be a product of generalised surveillance;

3. **Interventions must be lawful**: any investigation of private communications must have a specific legal basis, which must be publicly accessible, clear, precise, comprehensive and non-arbitrary. It must also comply with national and EU rules on due process, good administration, policing, accountability, transparency, non-discrimination and so forth;

4. **Interventions must be specifically warranted**: any investigation of private communications must be specifically and individually warranted by a judge. Police forces cannot enter a suspect's home or intercept phone calls without a warrant; the same principles apply to online private spaces. Warrants must be obtained before a person's communications are intercepted, and not retroactively;

5. **Measures must be the least privacy-invasive and limited to detecting CSAM only**: any investigation of private communications for detecting CSAM must guarantee that any interference with the right to privacy is as minimal as possible; restricted to detecting CSAM only; and that bias and accuracy are addressed to prevent discrimination and minimise the risk of false positives. In order to ensure this, national data protection authorities and the European Data Protection Board should provide mandatory guidance on the permissibility of specific technologies that are and will be used to detect CSAM;

6. **Independent oversight and scrutiny**: there must be rigorous oversight of existing and future technologies used for the detection of online CSAM by national data protection authorities, including: independent audits; enforcing reporting obligations on law enforcement in order to demonstrate the effectiveness of measures and enable scrutiny (such as on convictions, false positives, absolute vs repeat reports, and the services on which CSAM are detected); the proper undertaking of data protection impact assessments

(DPIAs) for all technologies / methods used; and transparency;

7. **Security**: independent security experts and civil society must have access to technical details of any proposed tools or technologies in order to assess intended or unintended risks. Measures that render devices insecure and vulnerable to malicious actors, such as Client Side Scanning (CSS), should not be allowed;

8. **Measures must protect encryption**: The availability and use of encryption is essential for the protection of our digital infrastructure and communications. Any measures to tackle CSAM must, therefore, respect encryption as a vital security measure and refrain from undermining its development, availability or use in ways that collaterally affect all users of the communications service. Methods like Client Side Scanning (CSS) undermine end-to-end (E2E) encryption by introducing means to circumvent cryptographic systems, which will inevitably be used by adversarial actors;

9. **Invest in tackling complex social issues in context**: the grave issue of child sexual abuse is not solely an issue of online dissemination. EU and Member States' responses to this serious problem must prioritise and invest in prevention, education, victim support, social services, welfare and other methods of addressing the root causes of the issues. Technological fixes are not a panacea to complex societal problems. Furthermore, the European Parliament's 2017 report on Member States' implementation of the Directive on combating child sexual abuse and exploitation, and the European Commission's 2020 Communication for a more effective fight against child abuse, both outline a number of important initiatives that Member States are yet to implement, and which should be remedied before suggesting new technical solutions or legislation.[5]

10. **Multi-stakeholder dialogue**: it is vital that the right stakeholders are brought together to engage in productive discussions about tackling online CSAM. When it comes to risks to privacy and data protection, digital rights groups – including those that represent the digital rights of young people specifically – must be given due weight.

Vitally, the process by which these principles are translated into law must meet the **highest levels of respect for the democratic process**. Unlike what happened during negotiations on the temporary derogation, Members of the European Parliament (MEPs) must be given sufficient time and support to execute their vital role of scrutinising legislative proposals and holding the executive arm of the EU to account.

The above principles will support an assessment of the necessity and proportionality of any proposed measure to tackle online CSAM which, given the vast implications on the right to privacy and confidentiality of communications, must be demonstrated by the Commission to ensure the lawfulness and permissibility of *any* derogation from the ePrivacy Directive.

For further information, please contact Ella Jakubowska, Policy Advisor, EDRi
ella.jakubowska@edri.org | +32 474 05 77 44

5 https://www.europarl.europa.eu/doceo/document/A-8-2017-0368_EN.pdf; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0607&qid=1634899236324