

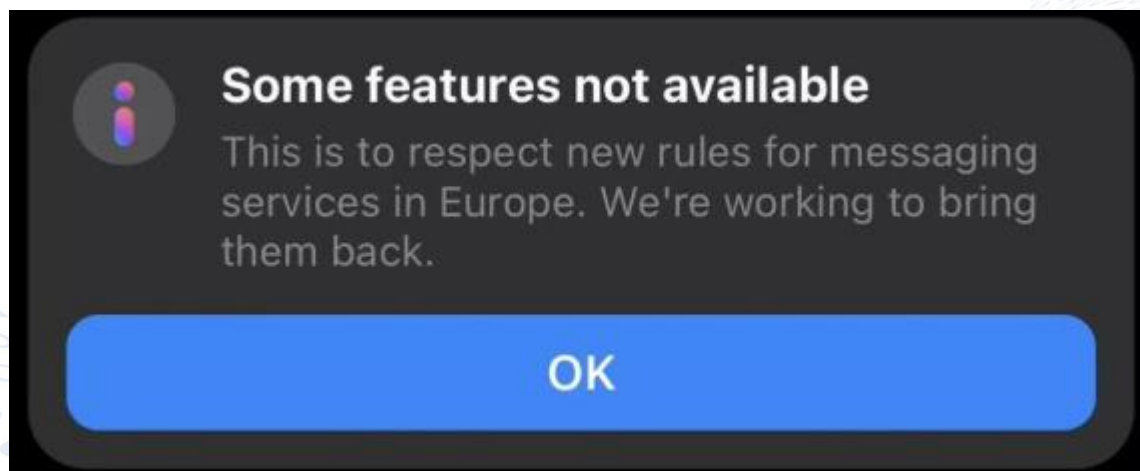


Confidentiality of communications and the fight against child sexual abuse online

Brendan Van Alsenoy
CIF Seminar series
19 January 2021

Background

- Extended scope EECC as from December 2020



→ Messaging, VOIP, web-based email service become subject to ePrivacy Directive, incl. rules on confidentiality (art. 5) and traffic data (art. 6)




Brussels, 24.7.2020
COM(2020) 607 final

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL
COMMITTEE AND THE COMMITTEE OF THE REGIONS**

EU strategy for a more effective fight against child sexual abuse

PhotoDNA

 Microsoft | **PhotoDNA** [PhotoDNA Cloud Service](#) [FAQ](#) [Documentation](#) [Terms of Use](#)

Help stop the spread of child exploitation

In 2009, Microsoft partnered with Dartmouth College to develop PhotoDNA, a technology that aids in finding and removing known images of child exploitation. Today, PhotoDNA is used by organizations around the world and has assisted in the detection, disruption, and reporting of millions of child exploitation images.



COM(2020) 568

Interim Regulation on the processing of personal and other data for the purpose of combatting child sexual abuse

Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online.



EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 7/2020

**on the Proposal for
temporary derogations
from Directive
2002/58/EC for the
purpose of combatting
child sexual abuse
online**

Child Sexual Abuse Directive (2011/93/EU)

- Requires following intentional conduct to be punishable:
 - *intentionally and knowingly obtaining access, by means of ICT, to child pornography;*
 - *distribution, dissemination or transmission of child pornography;*
 - *offering, supplying or making available child pornography*
- Requires MS measures to ensure prompt removal of webpages containing or disseminating child pornography
- Allows MS measures to block access to web pages containing or disseminating child pornography

Main recommendations

- Issues **not specific to fight against CSAM** online
- **Voluntary measures** also constitute interference
- Not relevant that merely seeks to allow « continuation » of existing voluntary practices
- Must comply with **Article 52 CFEU**

Specific recommendations

Lawfulness of processing

- make explicit whether derogation is intended to provide GDPR legal basis or not

Necessity and proportionality

- Cf. *La QDN* a.o, [ECLI:EU:C:2020:791](#), at para 121 et seq + [EDPS Guidelines on assessing proportionality](#)
- « PhotoDNA » vs. grooming detection based on keyword analysis

Specific recommendations

Scope and extent of derogation

- « NIICS » includes variety of services – all of them?
- Types of detection measures - « well-established » technologies?

Purpose and storage limitation

- Categories of data to be collected/retained/reported?
- Which recipients (« other relevant public authorities »)?
- When to report? How long to retain?

Specific recommendations

Reporting to relevant authorities

- Variety of DS: content providers, users, « suspects », victims
- What is confirmation process?
- Who manages/oversees relevant databases?

Transparency and data subject rights

- Any restrictions should comply with A23(1)-(2) GDPR
- Compare Proposal for Regulation on Terrorist Content

Specific recommendations

DPIA – prior consultation

- « without prejudice » does not suffice
- regulatory guidance is not a substitute for legality

Duration of the derogation

- temporary derogation should not exceed 2 years

CONCLUSION:

Proposal requires additional safeguards

Looking ahead

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

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 to communications between companies and their customers, and to work with governments to address these challenges.

- Embed the safety of the public activity effectively with no compromise safeguarding the vulnerable
- Enable law enforcement access where necessary and proportionate
- Engage in consultation with civil society and genuinely influences decisions



Global
Encryption
Coalition

[Home](#) [About](#) [Members](#) [Events](#) [News](#) [Take Action](#) [Join the Coalition](#)

[ENCRIPTION](#)

CDT, GPD and Internet Society Reject Time-Worn Argument for Encryption Backdoors

Thank you for your attention!

For more information:

Full text of Opinion 7/2020

www.edps.europa.eu

edps@edps.europa.eu



@EU_EDPS