EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

ePrivacy update - September 2020

Key developments

- The **DE Presidency** considers a General Approach may be feasible by the end of the year, provided Member States can come to an agreement on articles 6 (processing of metadata) and 8 (confidentiality of communications)
- Publication of the **EU strategy for a more effective fight against child sexual abuse**, containing several initiatives with impact on ePrivacy
- The Commission is actively looking for solutions which could allow companies to **detect and report child sexual abuse in end-to-end encrypted electronic communications**
- The Commission has published a draft **proposal for a temporary derogation** from certain provisions of the ePrivacy Directive to combat child sexual abuse online

LTT

- Confidentiality of communications is a cornerstone of the fundamental rights to privacy and data protection. The issues at stake are **not specific to the fight against child abuse** but to any initiative aiming at collaboration of the private sector for law enforcement purposes.
- Even voluntary measures by private companies to report or prevent the dissemination of child abuse material (CAM) **constitute an interference** with the rights to respect for private life and (increasingly electronic) communications of the individuals concerned (users, perceived perpetrators and victims).
- However, such interferences and limitations on the exercise of the rights and freedoms mentioned **may be possible, but under certain conditions**: they must be provided for by law and respect the essence of those rights and freedoms. Subject to the **principle of proportionality**, limitations may be made only if they are necessary and **genuinely meet objectives of general interest** recognised by the Union or the need to protect the rights and freedoms of others (see Article 52(1) of the Charter).
- Therefore, appropriate **safeguards are necessary** to ensure that monitoring will only be done in a **strictly targeted** way and that misuse of this mechanism is prevented by **appropriate security** measures. There is a need for a **precise description** of who is enabled to collect and keep what types of information and under what specific **safeguards**. **Transparency** and **independent redress** possibilities available to individuals are other essential elements to be integrated.
- In the interest of legal certainty for all actors involved, **harmonised, clear and detailed procedures** for the reporting of CAM should be **provided by law**, as opposed to a purely voluntary approach.
- Individuals should be able to continue to use, and companies should be able to continue to offer **end-to-end encryption** (without 'back-doors') to protect their electronic communications. We have in many occasions argued that a general ban on effective

encryption to reach specific benefits would more widely compromise rights and freedoms, including physical life, freedom of speech and democracy.

- **Technical solutions** to monitor for the dissemination CAM should be **effective, proportionate and limited to what is strictly necessary**. Different tools may involve different degrees of invasiveness and only the least intrusive tools should be used.
- The impact on end-users privacy of any technical solution is dependent on data flows architecture and on the chosen **data governance framework** of which there is no information. Data governance should define, among other aspects, the entities responsible for ensuring the CAM databases integrity, the auditability of the system or the procedures to ensure the system's transparency.
- **Banning E2EE services will not make the E2EE technology disappear**. Criminals will prefer facing charges for using banned E2EE services than facing them for child abuse. Moreover, unless there is a worldwide ban, criminals would use service providers in countries where E2EE is *not* banned (e.g. if E2EE is not banned in Russia, all criminals could move to Telegram which is based in Russia).

BACKGROUND

State of Play

Since the last update (January 2020)[1], the **main developments** were the following:

21 February 2020 - The Croatian Presidency proposed modifications in articles 6 (processing of metadata) and 8 (confidentiality of end-user equipment) and the related recitals. For both articles, the most important modification was the **possibility of relying on legitimate interests** (subject to additional safeguards[2]).[3]

6 March 2020 - The Croatian Presidency publishes a consolidated text of the Council draft, with certain new modifications with regard to the scope and M2M and IoT services.

> N.B. issues of **child imagery** or **data retention** were not discussed under the Croatian Presidency. Given the mixed reactions of Member States, as well as the outbreak of the COVID-19 pandemic, subsequent deliberations in WP TELE were paused until the German Presidency.[4]

6 July 2020 - The German EU presidency puts forward policy options in view of the first WP TELE discussion under its Presidency (using the March 2020 text from the Croatian Presidency as the starting point). The Presidency considers that **a General Approach and/or mandate** for negotiations is possible, provided an agreement can be reached on article 6 and 8. The German presidency also noted that it **intends to discuss the issue of detection of child abuse imagery separately at a later date**, which is one of the other outstanding issues. Member States were expected to voice their opinions at the WP TELE meeting of July 13.

24 July 2020 - Commission Communication on the EU strategy for a more effective **fight against child sexual abuse**, mentioning several **initiatives with impact on ePrivacy**:

[1] See briefing: “Possible EDPS/EDPB statement on the ePrivacy proposal” of 28/01/2020.

[2] In particular the following safeguards were proposed : no sharing with third parties, unless the data are anonymised; the need to carry out an impact assessment and, where appropriate, consult a supervisory authority; the obligation to inform the end-users of the envisaged processing operations and to provide them with the right to object; the obligation to provide adequate technical and organisational measures, such as pseudonymisation or anonymization. Moreover, the legitimate interest ground cannot be used when the legitimate interests pursued by providers are overridden by interests or fundamental rights and freedoms of the end-users (for instance if the data or information are used to determine the nature or characteristics or the end-user or to build an individual profile of the end-user). The proposed text also provided for certain presumptions for when this would be the case.

[3] Member States' first reactions, in particular to the introduction of legitimate interests ground, were mixed. A number of Member States would prefer not to include this new ground and would prefer to maintain a closed list of permitted processing grounds. Others were positive about the new direction, as being more aligned with the GDPR. Some also proposed to re-introduce some of the deleted processing grounds as they were not convinced that those would be adequately covered by legitimate interests. Certain delegations asked for more clarity when it comes to information society services financed through advertising.

[4] See also the May 2020 Progress report.

- As from December 2020, the e-privacy Directive will have an extended scope as a result of the already adopted Electronic Communications Code. This Code **extends the scope of the e-Privacy Directive** to over the top (OTT) inter-personal communication services[5] such as messenger services and email. This **would prevent certain companies** (in the absence of national legislative measures adopted in accordance with Article 15(1) of the e-privacy Directive) **from continuing their own voluntary measures** for detection, removal and reporting of child sexual abuse online.[6]
- The Commission will **first propose a narrowly targeted legislative solution** with the sole objective of allowing current voluntary activities to continue after December 2020.[7] In a second stage, by Q2 2021, the Commission will propose the necessary legislation to tackle child sexual abuse online effectively including by **requiring relevant online services providers to detect** known child sexual abuse material and require them to **report** that material to public authorities.
- The Communication states that **end-to-end encryption**, while beneficial in ensuring privacy and security of communications, **facilitates the access to secure channels for perpetrators** where they can hide their actions from law enforcement, such as trading images and videos.[8] The Commission underlines that the use of encryption for criminal purposes needs **to be addressed through solutions which could allow companies to detect and report child sexual abuse in end-to-end encrypted electronic communications**. Any solution would need to ensure both the privacy of communications and the protection of children from sexual abuse and sexual exploitation, as well as the protection of the privacy of the children depicted in the child sexual abuse material.

  NB: Under the **EU Internet Forum[9]**, the Commission has **launched an expert process with industry to map and preliminarily assess**, by the end of 2020, **possible technical solutions** to detect and report child sexual abuse in end-to-end encrypted electronic

[5] OTT stands for 'Over The Top' and refers to any streaming service that delivers content over the internet. The service is delivered 'over the top' of another platform. The type of OTT service: video (Netflix), audio (Spotify), messaging services (WhatsApp, Telegram or Signal) and voice OTT services (Skype or WhatsApp).

[6] The ePrivacy Directive does not contain a legal basis for *voluntary* processing of content and traffic data for the purpose of detecting child sexual abuse. Providers can only apply such measures if based on a national legislative measure, that meets the requirements of Article 15 of the Directive (proportionality etc.), for restricting the right to confidentiality. In the absence of such legislative measures, measures to detect child sexual abuse undertaken by these providers, which process content or traffic data, would lack a legal basis.

[7] According to Politico, the Commission plans to adopt this week the first of two instruments to tackle child sexual abuse material online. As the Commission wants to make sure that the ECC does not affect the fight against child sexual abuse online, meaning the new rules will need to be applicable by the end of the year.

[8] The Communication also notes that offenders have become increasingly sophisticated in their use of technology and technical capabilities including **encryption** and **anonymity** (e.g. peer-to-peer file sharing and the use of darknet). This criminal activity creates problems for society in general and for law enforcement in particular in its role of protecting society. The Communication also cites Facebook' plans to implement **end-to-end encryption** by default in its instant messaging service. In the absence of accompanying measures, it is estimated that this could reduce the number of total reports of child sexual abuse in the EU (and globally) by more than half and as much as two-thirds, since the detection tools as currently used do not work on end-to-end encrypted communications.

[9] The forum, which brings together all EU Home Affairs Ministers, high-level representatives of major internet companies, the European Parliament and Europol, has served since 2015 as a model for a successful cross-sector collaboration in the fight against terrorist content online and has now expanded to also cover child sexual abuse online

communications.[10] On 7 September 2020, Politico published an internal Commission document outlining possible solutions with the aim of gathering further expert input.

- Finally, Commission also announced the **possible creation of a European centre** to prevent and counter child sexual abuse. One of the centre's functions is to support companies by, for example, **maintaining a single database in the EU of known child sexual abuse material** to facilitate its detection in companies' systems, in compliance with EU data protection rules. In addition, the centre could also support law enforcement by coordinating and facilitating the takedown of child sexual abuse material online identified through **hotlines**. The centre could also **support victims in removing their images and videos** to safeguard their privacy, including through **proactively searching** materials online and notifying companies.

10 September 2020 - Commission publishes a proposal for an **Interim Regulation on the processing of personal and other data for the purpose of combatting child sexual abuse**, which:

- provides for a temporary derogation (4 years) from articles 5(1) (confidentiality of communications) and 6 (traffic data) of Directive 2002/58/EC;
- the derogation applies in connection with the provision of 'number-independent interpersonal communications services'[11] (e.g., voice over IP, messaging and web-based e-mail services) strictly necessary for the use of technology for the sole purpose of
  - ***removing*** child sexual abuse material and
  - ***detecting*** or ***reporting*** child sexual abuse online to law enforcement authorities and to organisations acting in the public interest against child sexual abuse

[10] Technical experts from academia, industry, public authorities and civil society organisations will examine possible solutions focused on the device, the server and the encryption protocol that could ensure the privacy and security of electronic communications and the protection of children from sexual abuse and sexual exploitation. The expert process should also help to address regulatory and operational challenges and opportunities in the fight against these crimes.

[11] Article 2 (5) EECC defines an '**interpersonal communications service**' as "a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service". A '**number-independent interpersonal communications service**' means an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans (Article 2(7) ECC).

Combatting child abuse while preserving ePrivacy and encryption

1. EDPS 2010 Opinion

In 2010, the EDPS issued an own-initiative Opinion on the on the proposal for a Directive on combating the sexual abuse, sexual exploitation of children and child pornography (now Directive 2011/93).

In his Opinion, the EDPS highlighted two data protection aspects that are **not specific to the fight against child abuse** but to any initiative aiming at the **collaboration of the private sector for law enforcement** purposes:

1. Private efforts to block the dissemination of child abuse material **involves surveillance and processing of personal data** of various individuals, be it information about victims, witnesses, users or content providers. Such monitoring amounts to an interference with their rights to respect for their private life and their correspondence. Considering this interference, more **appropriate safeguards are needed** to ensure that monitoring and/or blocking will only be done in a **strictly targeted** way and **under judicial control**, and that misuse of this mechanism is prevented by **adequate security** measures.

2. When it comes to **reporting**, there is a need for a **precise description** of what should be considered as illegal or harmful content, **who is enabled to collect and keep** information and under what specific **safeguards**. This is particularly important considering the consequences of reporting: in addition to the information related to children, personal data of any individual connected in some way with the information circulating on the network could be at stake, including for instance information on a person suspected of misbehaviour, be it an internet user or a content provider, but also information on a person reporting a suspicious content or the victim of the abuse. In terms of **quality and integrity** requirements, additional safeguards should be implemented in order to guarantee that this information considered as digital evidence has been properly collected and preserved and will therefore be admissible before a court. Guarantees related to the **supervision** of the system, in principle by law enforcement authorities, are decisive elements to comply with. **Transparency** and **independent redress** possibilities available to individuals are other essential elements to be integrated in such a scheme.

It should be noted that the EDPS **questioned purely voluntary mechanisms** to combat the dissemination of child abuse material, given the nature of the interference and the need for legal certainty for all actors involved. There is a need to ensure **harmonised, clear and detailed procedures** when fighting illegal content, under the supervision of independent public authorities.

Finally, it should be noted that **different tools may involve different degrees of invasiveness**. According to McIntyre, would be desirable to assess individual measures with regard to their invasiveness and to reaffirm the principles of proportionality and necessity so that more invasive systems (such as the scanning of email) should only be used if it can be shown that less invasive systems (such as blocking of public web sites) would not achieve the desired goals.

2. Encryption

a) <u>EDPS position on encryption</u>

The EDPS considers that the ePrivacy Regulation should clearly **allow users to use end-to-end encryption**[12] (without 'back-doors') to protect their electronic communications. Moreover, decryption, reverse engineering or monitoring of communications protected by encryption should be prohibited.

In addition, the use of end-to-end encryption should also be encouraged and when necessary, mandated, in accordance with the principle of data protection by design. In this context, measures to encourage development of technical standards on encryption should be considered[13].

The EDPS considers that the ePrivacy Regulation should **specifically prohibit encryption providers, communications service providers and all other organisations** (at all levels of the supply chain) **from** allowing or facilitating **'exceptional access keys' and 'back-doors'**. Systems with exceptional access to keys or with backdoors could make communications more complex and less secure.

Moreover, **backdoors** can be used for illegitimate purposes and can be also problematic with regards to the GDPR, in particular in relation to:

- **data protection principles** (under Article 5 GDPR, personal data processing must be fair, transparent and secure);

- the **responsibility of data controllers** (i.e. under Articles 5 and 24 GDPR, data controllers are responsible for compliance with data protection principles and must implement "appropriate technical and organisational measures" to ensure that processing is performed in accordance with the GDPR) and **processors** (i.e.under Article 28 GDPR, data processors must follow the instructions of controllers which are laid down in a binding contract with the controller); and is more likely to result in a "**high risk**" for the rights and freedoms of individuals[14].

[12] End-to-end encryption (E2EE) is a method of secure communication that prevents third-parties from accessing data while it's transferred from one end system or device to another. In E2EE, the data is encrypted on the sender's system or device and only the recipient is able to decrypt it.

[13] EDPS Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation) from 24 of April 2017, p. 34-35 https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

[14] See also Report from the IPEN workshops on encryption - what is encryption and who needs it for what? From 23 July 2020, https://edps.europa.eu/press-publications/press-news/blog/report-ipen-workshops-encryption-what-encryption-and-who-needs-it_en

b) *Statement of the WP29 on encryption*

In April 2018, WP29 published at a Statement on encryption, stating that

- the availability of **strong and efficient encryption is a necessity** in order to guarantee the protection of individuals with regard to the confidentiality and integrity of their data which is indispensable for **trust in the digital economy**.
- When data is transferred via the open internet, **encryption should ideally always cover the entire communication, from the device of the sender to that of the recipient (end-to-end-encryption)**.
- There is also a public interest in the implementation of encryption. Securing personal data in transit and at rest is a **cornerstone of the trust** we all need for digital services, so as to enable innovation and growth for our **digital economy**.
- **Backdoors** (i.e. vulnerabilities secretly implemented in a particular software by its developer) and **master keys** (i.e. keys allowing the decryption of every message encrypted with a specific software) deprive encryption of its utility **and cannot be used in a secure manner.** Any obligation aiming at reducing the effectiveness of encryption in order to allow law enforcement access to encrypted data could seriously harm the privacy of European citizens.
- **Law enforcement agencies already have a number of legal powers and targeted tools to address the challenge of encryption**, allowing them to access the data they need to investigate and prosecute criminals. In this context, the WP29 specifically mentions use of **specific and targeted tools to access documents before encryption on the sender's device, or after decryption by the recipient.**

c) *EDPB response to MEP Körner*

On 16 June 2020, in response to a question from MEP Körner, the EDBP stated that any ban on encryption or provisions weakening encryption would undermine the GDPR obligations on the concerned controllers and processors for an effective implementation of both data protection principles and the appropriate technical and organisational measures.

Similar considerations apply to transfers to controllers or processors in any third countries adopting such bans or provisions.

d) *European Electronic Communications Code*

The EECC emphasises the importance of encryption for security, while at the same time recognising the needs of law enforcement. It states that e-communications network and service providers should inform users of *'measures they can take to protect the security of their communications'* including using *'encryption technologies'*[15], and – **without prejudice to**

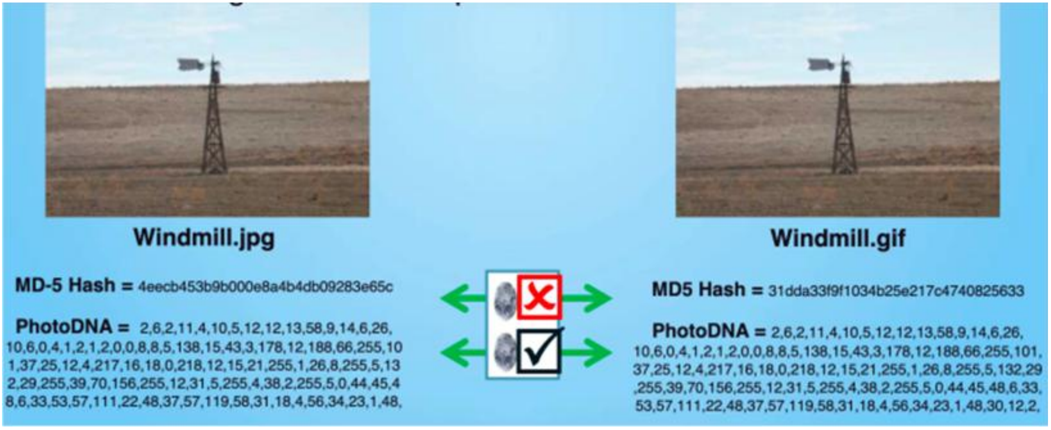
[15] Art. 40(1) EECC: *"Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Having*

criminal investigations[16] – states that encryption, ***'end-to-end where appropriate', 'should be promoted and where necessary, encryption should be mandatory'.***

Technical solutions under consideration

PhotoDNA and the US model

PhotoDNA is a technology developed by Microsoft and Dr. Hany Farid. It derives a short fingerprint that is designed to closely summarize a photograph. Unlike cryptographic hashing, which is sensitive to even the tiniest changes in a file, PhotoDNA fingerprints are designed to be robust even against complex image transformations like re-encoding or resizing.

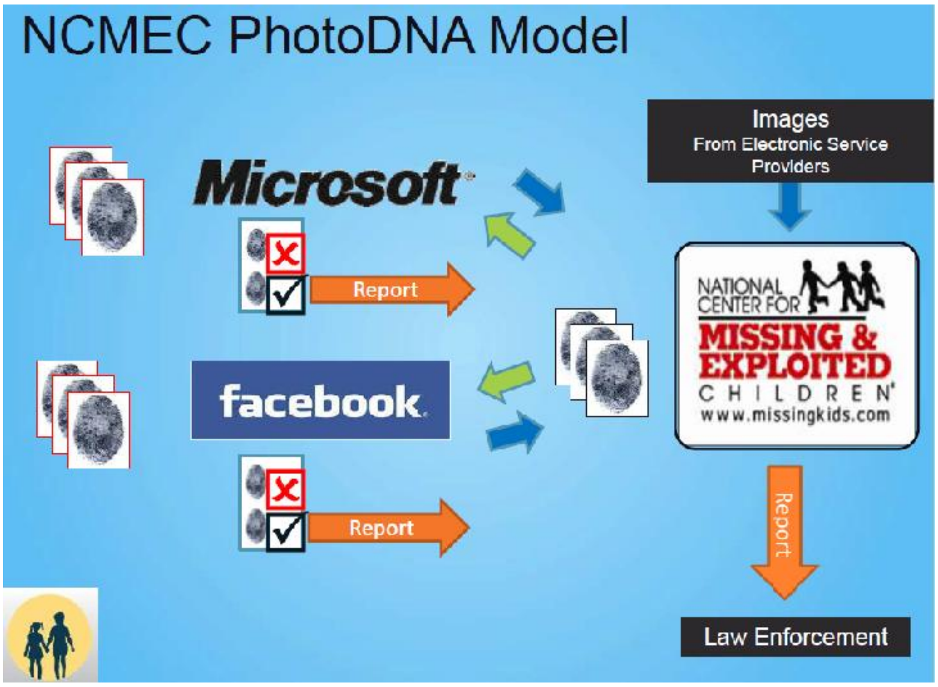

Windmill.jpg
MD-5 Hash = 4eecb453b9b000e8a4b4db09283e65c
PhotoDNA = 2,6,2,11,4,10,5,12,12,13,58,9,14,6,26,10,6,0,4,1,2,1,2,0,0,8,8,5,138,15,43,3,178,12,188,66,255,101,37,25,12,4,217,16,18,0,218,12,15,21,255,1,26,8,255,5,132,29,255,39,70,156,255,12,31,5,255,4,38,2,255,5,0,44,45,48,6,33,53,57,111,22,48,37,57,119,58,31,18,4,56,34,23,1,48,
Windmill.gif
MD5 Hash = 31dda33f9f1034b25e217c4740825633
PhotoDNA = 2,6,2,11,4,10,5,12,12,13,58,9,14,6,26,10,6,0,4,1,2,1,2,0,0,8,8,5,138,15,43,3,178,12,188,66,255,101,37,25,12,4,217,16,18,0,218,12,15,21,255,1,26,8,255,5,132,29,255,39,70,156,255,12,31,5,255,4,38,2,255,5,0,44,45,48,6,33,53,57,111,22,48,37,57,119,58,31,18,4,56,34,23,1,48,30,12,2,

PhotoDNA hashing (source: Microsoft)
Note that the hashes aren't identical. PhotoDNA uses a similarity metric to determine whether an image is a likely match.

U.S. federal law requires that U.S.-based ESPs report instances of apparent child pornography that they become aware of on their systems to the CyberTipline, the reporting system of the US National Centre for Missing and Exploited Children (NCMEC). To date, over 1,400 companies are registered to make reports to NCMEC's and, in addition to making reports, these companies also receive notices from NCMEC about suspected CSAM on their servers.

regard to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures, ***including encryption where appropriate****, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services";*

[16] Recital 97 of the Code highlights that *"[i]n order to safeguard security of networks and services, and without prejudice to the Member States' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences, the use of encryption for example, end-to-end where appropriate, should be promoted and, where necessary, encryption should be mandatory in accordance with the principles of security and privacy by default and by design."*



NCMEC PhotoDNA Model

Images
From Electronic Service Providers
Microsoft
Report
facebook
Report
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
www.missingkids.com
Report
Law Enforcement

Although the NCMEC 2019 report includes only US companies, the Commission's leaked report says 800K CAM reports concerned the EU.

The technical details of how PhotoDNA works are not public, most likely to prevent criminals learning how to avoid it. Dr. Hany Farid claims PhotoDNA has an expected error rate of approximately 1 in 50 billion[17].

In order to use PhotoDNA, electronic communication service providers (ECSP) need to access the content of the communication. End-to-end encryption prevents ECSPs (or anyone but the sender and recipient) from accessing the communication data. Therefore, end-to-end encryption renders useless PhotoDNA.

While the technology was developed with CAM in mind, since 2016, Facebook uses photoDNA to detect and remove violent terrorist imagery or terrorist recruitment videos or images.

Even if the Commission's leaked document does not mention PhotoDNA, it is very likely to be the hashing technology of choice since it was the source of 95% of the CAM reports in 2018[17].

[17] Hearing on the U.S. Congress House Committee on Energy and Commerce "Fostering a Healthier Internet to Protect Consumers" Professor Hany Farid, University of California, Berkeley. https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Farid.pdf

(Leaked) Commission document on "Technical solutions to detect child sexual abuse in end-to-end communications"

The document groups solutions four categories:

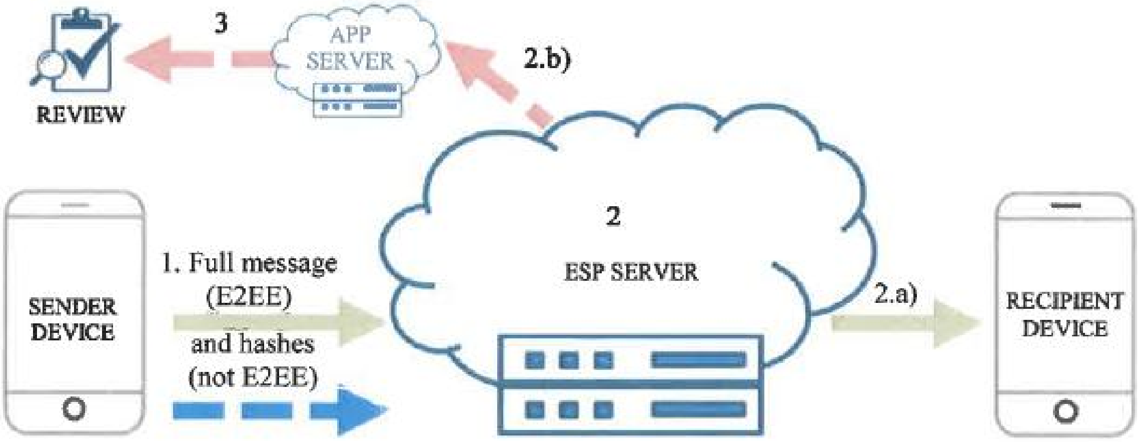
0. Baseline solutions
1. Device related solutions
2. Server related solutions
3. Encryption related solutions

Baseline solutions (not really considered as such in the report) are:

a. Not E2EE communications
b. Not detecting CAM in E2EE communications
c. E2EE communications with exceptional access (aka master keys)

In the short term, the report recommends two device related solutions:

1b) On-device full hashing with matching at the server



The user's device calculates the hash before encrypting the image or video and sends it to the Electronic Service Provider through a parallel communication channel (blue line).

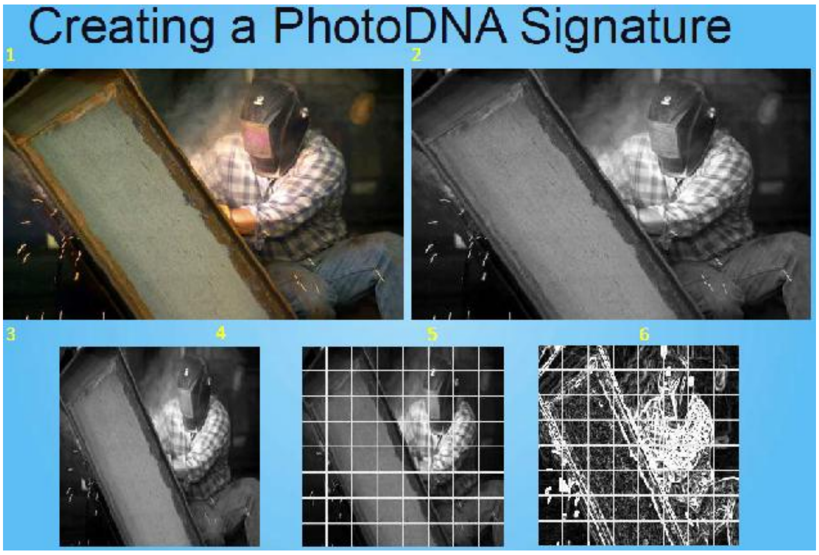
1c) On-device partial hashing with matching at the server
The difference with the previous option is that the device makes part of the calculation of the hash and the ESP server the other part. The aim is to reduce the risk of the device being manipulated to send a false hash.

The report does not specify how much information of the image or video gets the ESP, which is very relevant to assess this option's impact on privacy.

Issues and concerns related to the recommended solutions:

- **Generalised surveillance:** The technical solutions proposed in the document "Technical solutions to detect child sexual abuse in end-to-end communications" check all images uploaded or transferred by all users, thus **treating all users as suspects**. It is the **exact of opposite of a targeted approach**.

- **Proportionality**: In 2019, there were 16.8 million reports that included **69.1 million CAM files**[18]. Facebook platforms accounted for 94% of the reports. The estimated number of uploaded photos in 2019 using just[19] Facebook messenger[20] is **204 billion**. Even if we assume all files where found on Facebook messenger, **almost 3.000 photos have to be checked to find each CAM file**.
- The recommended technical solutions **bypass the user intention** of communicating privately (note the double arrows exiting the senders device in figures 5 and 6 in the document "Technical solutions to detect child sexual abuse in end-to-end communications").
- Both solutions' security relies on obscurity (hiding the processing in your device so the criminals will not find a way to avoid it), which will very likely lead to a lack of transparency.
- Both options reveal to the ESP the hashes of the images and videos. ESPs could build databases with hashes of other type of content (e.g. political images or videos) and check the hashes send by the device against those new databases to learn about the content exchanged.
- Option 1b) is vulnerable to device tampering, which criminals will probably do. That will lead to a surveyed general population while criminals avoid surveillance.
- Option 1c) reveals to the ESP not only the hash, but also partial information on the image video. The report does not specify how much information of the image or video gets the ESP, which is very relevant to assess this option's impact on privacy. See below an example of the process.



[18] NCMEC's exploited children statistics https://www.missingkids.org/footer/media/keyfacts

[19] Facebook owns also WhatsApp, but it implements E2EE connectivity so it can only check profile photos.

[20] 17 billion photos uploaded each month (Source).

All the long-term solutions recommended in the report (1d, 2a, 2c and 3a) need research, meaning that they cannot be deployed today. The legislator should not draft legislation thinking on applying certain technology that, when the legislation is passed, is not mature.

Initial assessment of the latest Council proposals for the ePrivacy Regulation

1. Permitted processing of metadata (article 6)

a) *Vital interests*

The German Presidency asks whether provisions allowing companies to process metadata without the users' consent because it is necessary to protect the vital interest of a natural person should be kept as is (option 1) or be revised to make it more aligned with the EU's General Data Protection Regulation (option 2).

In case of option 2, a new recital would be added which would clarify inter alia that processing of metadata for the protection of vital interests may include for instance processing necessary for humanitarian purposes, including for monitoring epidemics and their spread or in humanitarian emergencies, in particular natural and man-made disasters.

--> We would generally prefer the current wording[21] (option 1) as it is more clear regarding the circumstances in which metadata may be processed for purposes of protecting vital interests.

--> The new recital under option 2 also seems like a useful clarification, albeit that certain processing activities may be better justified by reference to "public health" rather than "vital interests", taking into account existing WP29 guidance.

In case of use of communication metadata for humanitarian purposes or epidemic fighting, service providers should also be required to comply with the purpose limitation, data minimization and storage limitation principles.

b) *Legitimate interests and statistical counting*

The German Presidency asks whether to keep the provision authorising the processing of metadata on the basis of legitimate interests subject to specific conditions and safeguards (option 1) or to remove this provision (option 2).

In case of option 2, the DE Presidency proposes a text which combines previous versions of the FI and BG Presidency. Processing of metadata for purposes of statistical counting would still be authorised (with a further distinction depending on whether the metadata also constitutes location data).

--> We would generally prefer option 2, again with a view of seeing legitimate interest removed as a legal basis.

[21] *"'(d) it is necessary to protect the vital interest of a natural person, in the case of emergency, in general upon request of a public authority, in accordance with Union or Member State law; or"*

The use of metadata for the purposes foreseen in Art. 6b(1)(a) (network management and optimization) and Art. 6b(1)(b) (billing) is related to the EDPB response to the BEREC request for guidance on net neutrality rules (EDPS lead rapporteur). The ISPs want to process the visited URLs and domain names for network management and for zero-rating offers. In the EDPB response we stated “IAS service providers do not require information included in the transport layer payload (like domain names or URLs) to convey a communication on an electronic communication network.” These two provisions as they are written would allow ISP access to domain names and URL data for those purposes. If we want to prevent ISPs from accessing the URLs and domain names, the provision should limit the metadata processed for this purpose to those necessary for the ECS provider to convey the message.

The TECH ES discussed in length if domain names and URLs should be considered traffic data for ISPs. Our view, which was supported by most but not all DPAs, is that the URL or domain names are not necessary for ISPs since they can deliver the IP packets knowing just the IP address.

We would suggest adding a provision in Art. 6b in this line: “Except when the end-user concerned has given consent, the providers of electronic communications networks and services shall only process the metadata they need to convey the messages.”

On the provisions proposed for statistical counting **using metadata constituting location data** it should be pointed out that:

- As Montjoye has demonstrated, "with a spatial resolution equal to that given by the carrier's antennas, four spatio-temporal points are enough to uniquely identify 95% of the individuals". Therefore, pseudonimization of the location data is not as useful as one might think. **IF** location data is to be used for statistical counting, it should be generalized to ensure a very low re-identification risk (e.g. city, province or region).
- A first requirement reflecting data minimization could be added to the text of option 2: "the processing is limited to the minimum amount of data necessary for the purposes of statistical counting"
- For the reasons expressed in the first point, the second requirement should be modified to require deletion and not anonymization of location data.
- the last requirement could be modified to better express the purpose limitation "*the metadata processed for the purpose of statistical counting will not be used for any other purpose such us determining the nature or characteristics of an end-user or building a profile of an end-user*."

On the provision regarding the use of **other metadata** for statistical counting or research:

- the manner in which research and statistical counting are mixed in the current drafting is confusing
- in our pleading to the CJEU we said that metadata can be as revealing as content and that the difference between content and metadata is not always clear-cut. A server with a unique IP address can host more than one domain. The domain name is metadata necessary to convey the message but the ISP can deliver the message knowing just the IP address (and maybe the port number). Once the IP packets are in

the server, the hosting service provider will need the domain name or URL to convey the message.

2. Confidentiality of communications (article 8)

On Article 8, the German Presidency asks Member States to consider, if access to terminal devices should be permitted for the purpose of a legitimate interest subject to specific conditions and safeguards (option 1), how the security of the respective equipment can be ensured under these conditions, given that this approach would considerably facilitate the installation of software which is frequently seen as a major gateway for malicious software.

Alternatively, should the compromise proposal of the FI Presidency be supported (option 2) (i.e. without legitimate interest but with statistical counting and web audience measuring), the Presidency asks inter alia:

1. whether delegations agree that Article 8, together with Recitals 20 and 21, establishes rules that appropriately balance a high level of protection of end-users' privacy with the legitimate interests of online publishers,
2. whether delegations see a need to further discuss the provision in Article 8(1), especially with regard to requirements for access to terminal equipment in connection with IoT (e. g. automated and networked driving or in the health sector)

--> as there should be no possibility under the ePrivacy Regulation to access/store information in the end-user's terminal equipment, under the *"legitimate interest*" ground, option 2 should generally be preferred.

However, the recitals in question indicate that "*making access to website content provided without direct monetary payment dependent on the consent of the end-user to the storage and reading of cookies for additional purposes would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques*" (unless there is clear imbalance, e.g. the website of a public authority). It is also indicated that "*access to end-users' terminal equipment may also be necessary for providing an information society service, requested by the end-user, such as services provided to safeguard freedom of expression and information including for journalistic purposes, such as online newspaper or other press publications as defined in Article 2(4) of Directive (EU) 2019/790, that is wholly or mainly financed by advertising provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar techniques and has accepted such use.*"

In addition, it should be noted that there is no clear-cut definition of audience measuring and data collected for audience measuring can be easily crossed with other data for different purposes. For example, Google Analytics could be regarded as an audience measurement tool but Google recognizes that it also uses those data for advertisement purposes ((section of advertising cookies) "...Google Marketing Platform and Google Analytics cookies may also be used for this purpose ")

In relation to IoT, It might be good to make a distinction between rules for IoT devices that are linkable to an individual (e.g. smart home devices, connected vehicles or smartphones) and those which will not (e.g. connected sensors deployed in a forest or a factory).

Careful consideration should be given to the definition of statistical counting. Not needing consent to know how many of your visitors are using each browser type or support a given plugin that they need to access some content on your website seems reasonable.

Finally, there should be a requirement for the providers of web services (analytics, chat boxes, maps, etc.) or Software Development Kits (SDKs) to inform their customers about the data their products and services set and collect from the end-user devices. Website operators should not have to carry the burden of investigating whether the third party components embedded set or access data on their visitors' devices or to check if users data is transmitted to third parties. Those providing services used in conjunction with electronic communication services or information society services which set or collect data from end-users' devices should inform their customers (website operators) so they could choose privacy wisely and comply with the obligation to inform their end-users. The same transparency requirement should be applicable to those using the communication metadata (e.g. device fingerprinting) to single out and track users. When a service provider (e.g. an adExchange) is tracking end-users using data or metadata collected through a third party (e.g. a website or an app), it should provide the third party with the necessary information to comply with the requirements of the ePrivacy Regulation.

Possible EDPB statement

- During the Plenary of 2 September 2020, the DE SA expressed the concern that in the latest draft of the ePrivacy Regulation the role of DPAs and EDPB are to be significantly reduced. As the DE Presidency hopes to achieve a General Approach shortly, it has requested that the TECH ESG work on preparing a statement as quickly as possible.
- The FR SA (as coordinator) recognised that there may be need political signal from EDPB prior to finalisation of work at Council level, but proposes to first discuss this at ESG level
- Both the EDPB and EDPS have already publically taken position on the proposed ePrivacy Regulation and called upon the Council to finalise its negotiating position without further delay. To achieve the biggest impact, we should carefully choose the right moment to issue a further possible EDPS/EDPB statement.
- The members of the EDPB stressed the importance of adopting a political statement on this matter soon, before the end of the process at the Council, which will be followed by a more in-depth analysis once the draft is public. Additionally, the members of the EDPB highlighted the importance of liaising with the national authorities in this regard.
- Taking this into account, the members of the EDPB gave a mandate to the TECH ESG to work on a political statement before the Council adopts its position, followed by an in-depth assessment of the final draft once it is published.