NOTE TO THE FILE

ePrivacy new developments

1. PhotoDNA

a) What is PhotoDNA?

PhotoDNA is a technology developed by Microsoft. It creates a unique digital signature (known as a "hash") of an image which is then compared against signatures (hashes) of other photos to find copies of the same image. When matched with a database containing hashes of previously identified illegal images, PhotoDNA is a tool to help detect, disrupt and report the distribution of child exploitation material.

b) PhotoDNA and the proposed ePrivacy Regulation

In November 2018 more than 50 other child rights NGOs from across the European Union, have sent a letter[1] to EU President Jean-Claude Juncker asking for the EU to amend the wording of the proposed ePrivacy Regulation. In the letter, it was highlighted that the new rules in their current form are likely to seriously endanger the safety and well-being of children. Furthermore, that the proposed ePrivacy Regulation would make it difficult for businesses to deploy software that detects this kind of material in online traffic – so it can be flagged and removed. Consequently, the NGOs asked for a specific exemption so that this type of technology can still legally operate.

c) EDPS position

The vast majority of services using the technologies[2] such as PhotoDNA do not constitute an electronic communications service and thus would not fall under the scope of the ePrivacy Directive. However, the General Data Protection Regulation applies to those services.

Moreover, **the draft of the ePrivacy Regulation** as proposed by the Commission does **not include provisions that would impact existing mechanisms that allow for the identification and reporting of criminal acts of child sexual abuse material.** In particular, the proposed Regulation not define social networks or on-line posts as protected confidential "communications". The proposal also contains the provision that leaves to the Member States the right to restrict by way of a legislative measure the scope of the obligations and rights provided for in Article 5 to 8 of the Proposal, when such a restriction constitutes a necessary, appropriate and proportionate measure to safeguard one or more of the general public interests. This approach is in line with the ePrivacy Directive 2002/58/EC in force today and respects the principle of subsidiarity, key to EU law.

Furthermore, the adoption of the ePrivacy Regulation is also crucial to effectively protecting the fundamental rights to privacy and confidentiality of communications of the victims of child sexual abuse. As particularly vulnerable users of new online services, they also stand to benefit from robust guarantees for secure, private and confidential electronic communications.

[1] https://www.ecpat.org/wp-content/uploads/2018/12/Letter-to-EU.pdf

[2]For example, Facebook, Google and Microsoft use PhotoDNA technology to scan for unlawful images. None of these services are OTT services.

d) EC activities

The Commission in its recent Communication[3] 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.

2. End-to-end encryption

a) What is end-to-end encryption?

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.

b) EC activities on end-to-end encryption and child sexual abuse online

The introduction of end-to-end encryption, while beneficial in ensuring privacy and security of communications, also facilitates the access to secure channels for perpetrators where they can hide their actions from law enforcement, such as trading images and videos. The Commission in its recent Communication[4] 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.

Under the EU Internet Forum, **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 communications**, in full respect of fundamental rights and without creating new vulnerabilities criminals could exploit. 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.

c) EDPS position on on end-to-end encryption

The EDPS considers that the ePrivacy Regulation should clearly **allow users to use end-to-end encryption** (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[5].

---

[3] Communication from the Commission on the EU strategy for a more effective fight against child sexual abuse from 24 of July 2020, COM(2020) 607 final

[4] Communication from the Commission on the EU strategy for a more effective fight against child sexual abuse from 24 of July 2020, COM(2020) 607 final

[5] 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

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'**[6]. 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 the requirement to notify to the competent DPA personal data breaches that are likely to result in a "risk" for the rights and freedoms of individuals (article 33 GDPR)

– and to individuals those that can result in a "high risk" (Article 34 GDPR)[7].

3. Entry into application of Electronic Communications Code ('EECC') and implications for law enforcement access

a) Over the top (OTT) services and processing of data for the purpose of detecting child sexual abuse

As from December 2020, the e-Privacy Directive will have an extended scope as a result of the European Electronic Communications Code ('EECC')[8]. This Code **extends the scope of the e-Privacy Directive to over the top (OTT) inter-personal communication services**[9] such as messenger services and email. 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.**

In July 2020, **the Commission announced**[10] **that it would propose a narrowly-targeted legislative solution with the sole objective of allowing current voluntary activities to continue**. This solution would allow the time necessary for **the adoption by Q2 2021of a new longer-term legal framework** 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**.

6

[7]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

[8] Directive (EU) 2018/1972 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018

[9] 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).

[10] Communication from the Commission on the EU strategy for a more effective fight against child sexual abuse from 24 of July 2020, COM(2020) 607 final

b) End-to-end encryption services and measures to permit the investigation, detection and prosecution of criminal offences

The **EECC does not prevent Member States from taking necessary measures to permit the investigation, detection and prosecution of criminal offences**, as long as they take into account Articles 7, 8 and 11 of the Charter. But concerning encryption specifically, that Code rather emphasises its security-building aspect: 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'*[11], and – **without prejudice to criminal investigations**[12] – states that encryption, ***'end-to-end where appropriate', 'should be promoted and where necessary, encryption should be mandatory'***

4. Opinion of Advocate General Pitruzzella and law enforcement access

Advocate General Giovanni Pitruzzella recently presented his opinion on the Estonian data retention law, advising on how Member States may arrange the contentious retention of personal data for law enforcement purposes while keeping in line with Union law[13].

The Estonian Supreme Court, indeed, had doubts on the compatibility with EU law of the circumstances in which investigating authorities had access to that information. The Estonian Supreme Court raised the question of whether Art. 15(1) of Directive 2002/58/EC on privacy and electronic communications, read in the light of Arts. 7, 8, 11, and 52(1) CFR, must be interpreted as meaning that the categories of data concerned and the duration of the period for which access is sought are among the criteria for assessing the seriousness of the interference with fundamental rights that is associated with the access by competent national authorities to the personal data that providers of electronic communications services are obliged to retain under national legislation.

AG Pitruzzella confirmed this view. Examining the lessons learned from the judgments in Tele2 Sverige/Watson (Joined Cases C-203/15 and C-698/15, see eucrim 4/2016, p. 164) and Ministerio Fiscal (Case C-207/16, see eucrim 3/2019, pp. 155-157), the **AG concludes that both the categories of data concerned and the duration of the period for which access to these data is sought are relevant**. He further states that, **depending on the seriousness of the interference, it was up to the referring court to assess whether this access was strictly necessary to achieve the objective of preventing, investigating, detecting, and prosecuting criminal offences.**

Although not examining encrypted data, this case is important as it will reveal more broadly how the Court of Justice will carry out **the balancing exercise between the need for data for the purposes of criminal prosecution vs data protection rights.**

---

[11] 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 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";*

[12] 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."*

[13] Opinion of Advocate General Pitruzzella in case C-746/18, H.K. v Prokuratuur, delivered on 21 January 2020 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CC0746