Child sexual abuse and the ePrivacy Regulation: Factsheet on the use of hashing technology

This paper provides information on hash technology used to detect and remove child sexual abuse material online, based on previously identified material[1]. The paper focuses on the use of such technology in electronic communications, as requested by Cabinets, to support reflections on the envisaged "standstill clause".[2] In 2018, more than 800,000 reports concerning instances of child sexual abuse in the EU were brought to the attention of law enforcement in the EU. More than 600,000 of those were detected in electronic communications systems.

The note first presents information on PhotoDNA. Developed by Microsoft and Professor Hany Farid, PhotoDNA is the main hash technology tool to detect child sexual abuse material across a variety of services[3] and serves as an example to illustrate how the detection process works. The note explains the reporting system in place today and provides information concerning the services in scope of the e-Privacy Regulation proposal and the volumes of notification.

Two annexes provide examples of actual cases from EU Member States' law enforcement agencies triggered by notifications based on automatic detection, as well as further technical details on how PhotoDNA works.

How PhotoDNA works

In a first step, PhotoDNA identifies images above a certain size. Then it creates a unique digital signature (known as a "hash") of the image. This hash is unique and irreversible, meaning that the image itself cannot be re-created from the hash. In a third step, the hash is compared against a database containing hashes of previously identified illegal child sexual abuse images. (It should be noted that, at the moment, PhotoDNA does not work with, and cannot detect images in, encrypted messages.) If there is no match, PhotoDNA immediately deletes the hash.

---

1 The sources of this document are the following (unless otherwise indicated):
- Microsoft website on PhotoDNA
- Call between DG HOME and Microsoft (PhotoDNA developer) on 7/2/2019.
- Discussion with Professor Farid, the main developer of PhotoDNA, on 5/3/2019, with DG HOME, CNECT H2, DG JUST and LS attending. Currently a Professor in the University of California at Berkeley, Professor Farid is an expert in digital forensics and image analysis who has provided expert witness testimony in US courts in more than 20 cases and expert testimony in the European Parliament in 2018.

2 This "standstill clause" is being considered in order to preserve the ability of over-the-top (OTT) providers (e.g. providers of webmail, VOIP or messenger services) to use hash technology for detection and removal of child sexual abuse materials in the context of electronic communications to the same extent as this may currently be permitted under the GDPR and other applicable European or national law. In the absence of this or another measure with comparable effect, the current practice of such providers would become unlawful under the new ePrivacy framework as of 21 December 2020, once the scope of the current ePrivacy Directive (or of the ePrivacy Regulation, if adopted by then) will be extended to OTTs.

3 According to Professor Farid, over 90% of the material referred to the National Center for Missing and Exploited Children is detected with PhotoDNA.

The tool focuses on images only and ignores text, i.e. it does not read the text of the email or extract any other information transmitted in the one-to-one message. It also cannot recognise faces in the images, or other contextual information. In other words, it does not answer the question "what is this message about?" but the question "has this image already been identified as depicting child sexual abuse?"

PhotoDNA has a high level of accuracy. The rate of **false positives** is estimated by Prof Farid at no more than 1 in 50 billion, based on testing. PhotoDNA has been in use for more than 10 years by over 150 organisations globally[4] including service providers (Microsoft, Facebook, Twitter, Apple[5]), NGOs (e.g. Internet Watch Foundation) and law enforcement in the EU (e.g. Europol, DE, SE and others). In these 10 years, the tool has been used daily and analysed hundreds of billions of images without any accuracy concerns being identified.

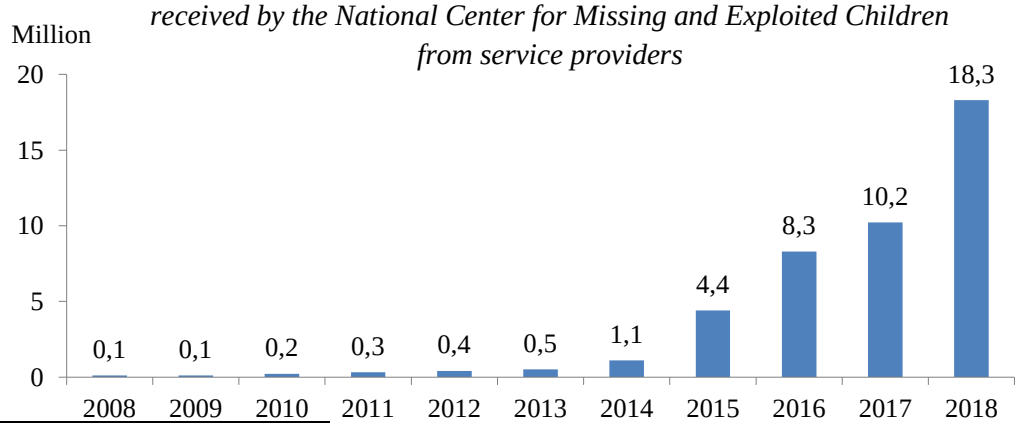
The reporting framework under US law

In the absence of a specific reporting framework for child sexual abuse materials under EU or Member States' law, a large volume of reports reaches EU Member States' authorities courtesy of reporting under US law. Under US law[6], if service providers choose to detect child sexual abuse materials voluntarily, they are required to report any detected material to the National Center for Missing and Exploited Children. This obligation does not distinguish between child sexual abuse materials that are made publicly available and materials that are shared in a private communication. The report includes content and metadata to identify the uploader/sender and the victim.

Number of notifications on the basis of automated detection

The overall number of reports has increased exponentially in the last years:

Figure 2: number of reports of child sexual abuse material received by the National Center for Missing and Exploited Children from service providers



[4] Microsoft provides PhotoDNA for free. Organisations wishing to use PhotoDNA must register and follow a vetting process by Microsoft to ensure that the tool is used by the right organisations for the exclusive purpose of detecting child sexual abuse material. The tool can be used to detect child sexual abuse material in various services (e.g. hosting, electronic communications) and devices (e.g. by law enforcement to detect known child sexual abuse material in a suspect's device).

[5] Apple has recently (May 2019) started to use PhotoDNA, see here.

[6] 18 U.S. Code § 2258A - Reporting requirements of electronic communication service providers and remote computing service providers.

- If the report refers to activity in the EU (e.g. uploaded/sent from an IP address in the EU), the National Centre for Missing and Exploited children sends it to the relevant law enforcement authorities in the EU.
- As a result, Europol and national law enforcement agencies in the **EU** received in 2018 **more than 800,000 reports** concerning instances of child sexual abuse in the EU[7].
- According to the Internet Watch Foundation, the country that hosts the largest amount of child sexual abuse material globally is in the EU (Netherlands)[8].
- Of the 18,3 million reports filed with NCMEC in 2018, **more than 10 million reports** concerned services under the scope of the e-Privacy proposal (i.e. messaging and email services), as reported by NCMEC.
- **More than 600,000** of these 10 million reports received in 2018 concerned situations in the **EU**[9], in which case they were channelled to law enforcement in Europe, as reported by NCMEC.

The filtering system has been acknowledged as an important contribution to law enforcement to help protect children in the EU from sexual abuse (including by law enforcement in NL, DE, ES, Europol and the German Special Rapporteur for the fight against Child Sexual Abuse).[10] In the absence of these filtering tools also being applied to electronic communications, it is possible that the volume of child sexual abuse material exchanged via the services under the e-Privacy proposal would increase, as offenders constantly look for ways that facilitate the exchange of this material with impunity.[11]

The Commission position on automatic detection of child sexual abuse materials

The Commission position on automatic detection tools such as PhotoDNA is set out in its 2017 Communication and 2018 Recommendation on tackling illegal content online[12]. In the 2017 Communication, the Commission "strongly encourages the further use and development of automatic technologies to prevent the re-appearance of illegal content online." In the 2018

7 As reported by NCMEC.

8 Internet Watch Foundation Annual Report 2017.

9 As reported by NCMEC.

10 See, e.g., https://www.europol.europa.eu/newsroom/news/international-police-action-leads-to-rescue-of-22-month-old-romanian-sex-abuse-victim; https://www.extremnews.com/nachrichten/vermischtes/d11216ab138a977; https://www.faz.net/aktuell/gesellschaft/kriminalitaet/meldepflicht-fuer-provider-nach-campingplatz-missbrauch-verlangt-16017398.html; https://www.policia.es/wap/prensa/20190427_1.html.

11 Inter alia, the UNODC Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children of May 2014 highlights the measures criminals take to evade detection by law enforcement (see, e.g., p. 33) https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf.

12 2017 Communication (COM(2017) 555).
2018 Recommendation (C(2018) 1177). The Global Alliance Against Child Sexual Abuse Online was launched by the European Commission and the US in 2012 and gathered 54 countries (including all Member States, since grown to 70 countries) to raise standards worldwide and unite efforts around the world to more effectively combat online sexual crimes against children.

Recommendation, the Commission again recognised that proactive measures, including by using automated means, can be an important element in tackling illegal content online, in particular if the illegal character of the content has already been established or where the type of content is such that contextualisation is not essential. This is the case of child sexual abuse material, for which the Commission stated in the Recommendation that service providers "should take proactive measures to detect and prevent the dissemination of such material, in line with the commitments undertaken in the context of the Global Alliance against Child Sexual Abuse Online."

Annex 1: Examples of actual cases concerning the services under the e-pPrivacy proposal Regulation[13]

Sample cases in Denmark:

- Case #1 - Operation Umbrella[14]:
  - In 2017 Facebook reported to NCMEC the distribution of videos via **Facebook Messenger**[15] depicting a Danish boy and girl who were engaged in sexual activity.
  - NCEMC forwarded the case to Denmark via Europol.
  - Over 1000 people had distributed the videos to one or more people via Facebook Messenger and were charged for distribution of child pornography.
  - This operation, still ongoing, is the single **largest operation ever** against child sexual abuse in Denmark.
- Case # 2:
  - Following reports from KIK alerting of the distribution of child sexual abuse material through **KIK Messenger**, Danish authorities arrested **on 10 April 2019**, a 41 year old Danish national with no criminal record.
  - During preliminary examination of his mobile phone, Danish police found several recordings of himself abusing his **10 year old daughter**.
  - The **10 year old victim was rescued** and the suspect is undergoing criminal proceedings.

Sample cases in Sweden

- Case # 1:
  - Swedish police received a NCMEC report alerting that one person had shared two child pornographic images on **Facebook Messenger** of material known to the police.
  - Swedish police carried out a search at the suspect's home and found child sexual abuse material in hard drives.
  - The material included the suspect **abusing his stepdaughter**, who was **rescued** in the operation.
  - The suspect was sentenced to nine years in prison for, among other things, gross rape against children.
- Case # 2:
  - Swedish police received a report from the National Child Exploitation Coordination Centre (Canadian equivalent to NCMEC) in which a person was sharing child sexual abuse material through **KIK Messenger**.
  - A house search was conducted in which child sexual abuse material was found.
  - Thanks to the investigation, **nine Swedish children** were identified.
  - The suspect was sentenced to four years in prison for different child pornography offenses.

---

13 Cases reported by law enforcement agencies in Member States or by the press in third countries.

14 This case was also included in the 2018 Internet Organised Crime Threat Assessment, p. 32, Europol.

15 The case was also reported in the media (in English).

- Case # 3:
  - Swedish police received in 2016 a NCMEC report submitted by Facebook concerning child sexual abuse material exchanged via **Facebook Messenger**.
  - The investigation revealed that a female suspect was producing child sexual abuse material with the children of her romantic partners and sharing it with another male.
  - Further investigation revealed a network of two other female producers and three male consumers of child sexual abuse material.
  - **11 victims** were identified and rescued, ranging from ages 2 to 14 when the crimes occurred, out of more than 50 victims in total.

Sample case in Ireland (Matthew Horan case[16])

- Law enforcement in Ireland received in 2013 a report from the National Center for Missing and Exploited Children alerting of the distribution of child sexual abuse material by **email**.
- The material was detected by Microsoft when Matthew Horan used a **Gmail** account to send child sexual abuse material to an email address on **Microsoft's** platform.
- The report led to an investigation in which it was discovered that Horan had been sexually exploiting children.
- Irish police identified **six victims** in Ireland as a result of the investigation.

Sample case in Romania[17]

- Romanian police received in 2016 a NCMEC report submitted by Facebook concerning child sexual abuse material exchanged via **Facebook Messenger**.
- The investigation revealed that a mother had been abusing her **9 year old daughter** for more than a year and sent the material generated in the sexual abuse to her boyfriend (not the father of the girl) in England.
- The mother was arrested and **her daughter was rescued**.

Sample case in Spain (Operation Corona)

- Law enforcement in Spain received in June 2016 a report from the National Center for Missing and Exploited Children alerting of the distribution of child sexual abuse material by **email**.
- The investigation by law enforcement in Spain led to the arrest of one person, who actively shared online with other child sex offenders the child sexual abuse material he produced.
- The person arrested produced that material by abusing children within his family circle.
- Given the gravity of the situation, law enforcement focused on locating the victims, eventually **rescuing two children** within the family circle from the ongoing abuse.

16 The case was also reported in the media.
17 The case was reported in the media, see here and here.

Sample cases in France:

- Case # 1:
    - French police received in 2018 a NCMEC report submitted by Facebook alerting of the distribution of child sexual abuse material via **Facebook Messenger**.
    - The investigation revealed that the offender provided **PlayStation codes** to young boys in exchange of child sexual abuse material.
    - The offender was arrested. There were around **100 victims**.
- Case # 2:
    - French police has received a number of cases from NCMEC submitted by KIK alerting of the distribution of child sexual abuse material via **KIK Messenger.**
    - The cases typically involve multiple offenders (up to **20 offenders** per case).
    - The cases have led to **multiple arrests**.

Sample case in Greece

- Greek police received two NCMEC reports submitted by Yahoo! informing about a user who exchanged child sexual abuse material via **Yahoo!'s messenger** service.
- The house search of the offender revealed that he was also in contact, via Skype, with individuals (mothers of underage children) in the ASEAN region and was sending money to them so they would send him indecent pictures of their underage children.
- The ASEAN authorities were notified of all the details.

Sample case in Bulgaria

- Law enforcement in Bulgaria received in 2018 a report from the National Child Exploitation Coordination Centre alerting of the distribution of child sexual abuse material through **KIK Messenger**.
- The report led to a criminal investigation in which two mobile phones from a suspect were seized, containing 517 video files with child sexual abuse material.
- The material included videos with **brutal scenes of child sexual abuse** with a child around **2 years old**.

Sample case in the Czech Republic

- Law enforcement in the Czech Republic received in 2017 a report from NCMEC alerting of the distribution of child sexual abuse material by **email**, initiated by **Google**.
- The report led to a criminal investigation in which a 52 year old man was arrested following a house search, where additional child sexual abuse material was found.
- This person had abused **2 girls** and recorded the abuse. The 2 girls were identified and rescued.

Sample case in Estonia

- Law enforcement in Estonia received in 2017 a report from NCMEC alerting of the distribution of child sexual abuse material by **email**.
- The report led to a criminal investigation in which a person was arrested for exchanging and possessing child sexual abuse material.

Sample case in the UK

- Law enforcement in the UK received a **Twitter** referral via NCMEC regarding the use of direct messages to send and receive child sexual abuse material.
- Following dissemination of an intelligence package to UK Police, the suspect was arrested.
- Safeguarding measures were taken in respect of the suspect's **3 children** who resided with him.

Europol echoed some of the above evidence by reporting in its 2018 Internet Organised Crime Threat Assessment on the various ways that child sexual exploitation material (CSEM) is distributed online, pointing out that "Some law enforcement agencies also see **traditional email services** being used to send and receive CSEM."[18]

Sample case is Switzerland

- Law enforcement in Switzerland received in 2016 a report from NCMEC alerting of the distribution of child sexual abuse material by **email**, initiated by **Google**.
- The report led to a criminal investigation in which a 45 year old man was arrested following a house search, where additional child sexual abuse material was found.
- The man was also suspected of **abusing his niece (child).** The suspect had also filmed minors secretly and provided the videos to other people.

Sample cases in the US

- Case # 1 (Kevin R. Hyde case)[19]:
  - US law enforcement received in 2017 a report from NCMEC submitted by **AOL** alerting that the owner of the email address tights.nylons2@aol.com had on at least 25 occasions sent an email to himself at three different IP addresses and which had images attached to them, many of which appeared to contain child sexual abuse.
  - The police alleged reviewed the thirteen videos and sixteen images included with the report and found that they depicted young girls ranging in age **from three years old to approximately ten years** old being vaginally and orally penetrated by adult males or had their genitals lewdly exhibited.
  - A search warrant was executed at the suspect's residence and various computer and
  - electronic equipment were seized. The suspect allegedly stated to police, in sum and substance, that tights.nylons2.aol.com was his email account, **that he created the account in 2015 for the purpose of downloading child pornography of**

[18] 2018 Internet Organised Crime Threat Assessment, p. 32, Europol.
[19] As reported in the press release from Queens District Attorney, see here.

children doing disgusting acts, that he would **email the images and videos to himself** to save, that he would trade images containing child exploitation with other individuals through his email and that he created another account to save the images.

- Case # 2 (Rev. W. Thomas Faucher case)[20]:
  - US law enforcement received in 2018 a report from NCMEC alerting of the distribution of child sexual abuse images by **email**.
  - The report led to a criminal investigation that revealed that the email account belonged to a retired Catholic priest who had expressed a desire to have sex with boys, had "satanic desires," and that "the thought of killing someone" was exciting to him.
  - More than 2,500 illegal files containing violent child pornography were recovered from Faucher's computer, cell phone, and Dropbox account. In some videos, the child victims wept as they were abused.
  - Authorities also revealed the priest shared his fantasies with other pedophiles online. He spoke of wanting to sexually abuse altar boys and babies. In one exchange, **he recalled enjoying a video of a boy being beaten to death**.
  - The Roman Catholic Diocese of Boise stated that "The **volumes of shocking information that the law enforcement investigation uncovered** reveal the **heinous nature of child pornography and the tragic impact upon its victims**"
- Case # 3 (Dabbs Postma case)[21]:
  - US law enforcement received in 2017 a report from NCMEC submitted by Facebook alerting of the exchange between two users via **Facebook Messenger** between Aug. 4 and Oct. 25 of **hundreds of photos and videos** containing child sexual abuse.
  - The report led to a criminal investigation in which Postma's home was searched. The police found a video showing him performing sex acts on **a young girl**.
  - Postma admitted to producing child pornography and having a sexual relationship with the girl, who was safeguarded.
- Case # 4 (Juan Rolando Lafuente case)[22]:
  - US law enforcement received in 2018 a report from NCMEC submitted by Facebook alerting of the exchange between two users via **Facebook Messenger** of child sexual abuse material.
  - The report led to a criminal investigation in which the police found in Lafuente's computer images of nude children performing sexual acts and in his phone videos of children engaging in sexual activity.
  - The suspect (59) was arrested and charged with two counts of possession of a photograph of sexual performance by a child and two counts of promoting pornography by a child.

[20] The case was reported in the press, see here.
[21] The case was reported in the press, see here.
[22] The case was reported in the press, see here.

- Case # 5 (Thomas William Barnes case)[23]:
  - US law enforcement received in 2017 a report from NCMEC submitted by **Yahoo** alerting of the sharing of child sexual abuse material via **email.**
  - The report led to a criminal investigation in which the police searched the suspect's computer and found multiple folders of child sexual abuse material.
  - The suspect, 67-year-old Thomas William Barnes, was a former spokesman for Florida's child welfare agency. He was charged with multiple counts related to child pornography.

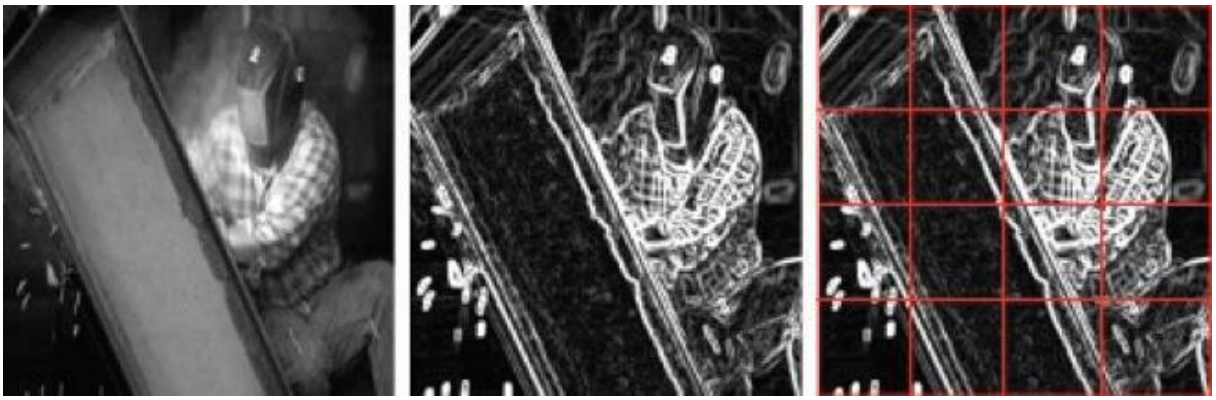
[23] The case was reported in the press, see here.

Annex 2: How PhotoDNA works (in detail)

1) Scanning:
   - The tool first identifies images above a certain size.
   - The tool focuses on images only and ignores text, i.e. it does not read the body of the email or extract any other information transmitted in the one-to-one message (it does not recognise faces in the images, or other contextual information). In other words, it does not answer the question "what is this message about?" but the question "is this image known?"
2) Creating the hash (see figure 1 below)[24], through the following process:
   1. Convert a full-resolution color image (top) to grayscale and lower resolution (bottom left);
   2. Use a high-pass filter to highlight salient image features (bottom center); and
   3. Partition the high-pass image into quadrants from which basic statistical measurements are extracted to form the PhotoDNA hash (bottom right).

Figure 1: hashing process

[24] Reining on online abuses, Farid, H., Dartmouth College, USA, 2018



- PhotoDNA hash is not reversible, and therefore cannot be used to recreate an image.

3) Matching:
   - The hash is compared with those in a database of hashes of known child sexual abuse material. If the image hash is not recognised, no information is kept.
   - Database[25]:
     - The main and largest database of hashes (around 1,5 million) is held by the National Center for Missing and Exploited Children, a public-interest, non-governmental organisation established by US Congress in 1984 to facilitate detection and reporting of child sexual abuse material[26].
     - The criteria for an image to be converted into a hash added to the database of the National Center for Missing and Exploited Children is the following:
       - Children (prepubescent or pubescent) engaged in sexual acts.
       - The sexual contact may involve the genitals, mouth, or digits of a perpetrator; or it may involve contact with a foreign object.
       - An animal involved in some form of sexual behaviour with a pre-pubescent child.
       - Lewd or lascivious exhibition of the genitalia or anus of a pre-pubescent child.
       - Images depicting pubescent children contain children that have been identified by law enforcement (therefore ensuring that they are actually minors).
     - Every hash has been viewed and agreed upon as being child sexual abuse material by two different experts at the National Center before it is included in the database.

[25] Source: National Center of Missing and Exploited Children.

[26] US providers may not able to use a database of hashes set up by law enforcement, as they could be accused of being a government actor and violate the Fourth Amendment to the US Constitution (protection against unreasonable searches and seizures).