OUTCOMES BRIEFING

Technology, privacy and rights: keeping children safe from child sexual exploitation and abuse online

Expert Roundtable Outcomes Briefing

Hosted by WePROTECT Global Alliance in partnership with ECPAT International

8 April 2021

The contents of this paper reflects the discussion had by participants. They do not necessarily represent the views of members of the WePROTECT Global Alliance or of ECPAT International.

1. Context

a. This roundtable, in partnership with ECPAT International, was the first in a new series of gatherings hosted by WePROTECT Global Alliance. It emerged in response to the controversy surrounding the European Commission's proposal for a temporary derogation to the e-Privacy Directive[1] and the Electronic Communications Code[2]. This has shone a spotlight on the challenges inherent in balancing privacy with child protection, as well as the need for consensus on the proportionate use of innovative technology by private companies to proactively identify children at risk of or experiencing exploitation and abuse.

b. This debate has also highlighted the need for careful consideration of proposals for long-term legislation and structures that ensure a robust system for preventing and responding to child sexual exploitation and abuse (CSEA) in digital environments, including through regulation of digital service providers, without undermining fundamental rights.

c. A group of experts representing various sectors, including data protection, privacy, AI and technology, child rights and victim support, were invited to explore the legal basis for use of tools to detect CSEA online, and discuss the privacy and child safety implications of these tools from different perspectives.

d. The primary objectives were to identify common ground and to identify solutions that sufficiently balance the rights of all users of the internet and the specific rights of children, in particular victims of CSEA online.

e. Three key discussion questions guided the debate:
   i. Does existing legislation in Europe (and the US) provide a robust framework for online detection tools?
   ii. What can we learn from the implementation of existing cybersecurity tools?
   iii. Is there identifiable common ground between privacy and child protection advocates?

f. Discussion was also built on the premise that arguments need to be evidence-based in terms of legislation and the functionality of the tools both specifically and generically. Therefore, the discussion was grounded with an opinion on the legal basis in the GDPR for the use of technology to detect known child sexual abuse material (CSAM).

g. While acknowledging that legal opinions can be made to support different sides of this debate, there are strong arguments to support the position that service providers can base the processing of personal data in the context of detecting and reporting CSAM on either a task carried out in the public interest (Art. 6.1 (e) GDPR) or on legitimate interest (Art. 6.1 (f) GDPR). The former legal basis requires a provision in Union or Member State law in which this public task is set forth or can at least be based on. The national transposition of Article 16.2 CSA Directive may provide such a provision. That same provision can then be used to invoke reasons of substantial public interest (Art. 9.2 (g) GDPR) to obtain an exemption from the prohibition of processing special categories of personal data.

h. Because the ePrivacy Directive prevails over the GDPR with regards the processing of confidential information by providers of Number Independent-Interpersonal Communications Services (NI-ICS), a derogation enables service providers that offer a range of online services to use a more holistic, cross-service approach to ensure compliance with data protection law while taking efficient action against CSEA online.

i. This addresses in part to the opinion of the European Data Protection Supervisor on the interim derogation, that: *"Confidentiality of communications is a cornerstone of the fundamental rights to respect for private and family life. Even voluntary measures by private companies constitute an interference with these rights when the measures involve the monitoring and analysis of the content of communications and processing of personal data. In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measures in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse."*[3]

1 – https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

2 – COM_COM(2020)0568_EN.pdf (europa.eu)

3 – https://edps.europa.eu/data-protection/our-work/publications/opinions/opinion-proposal-temporary-derogations-directive_en

2. Key challenges

There is insufficient transparency, trust and accountability around the nature and proportional use of tools to detect CSEA online.

a. It was argued that the GDPR offers a robust framework to allow the use of automated tools that detect, remove and report CSEA online. However, fundamental rights must be looked at in the round to ensure the right to privacy is also regarded. Fundamental rights apply equally to children as they do to adults, although special attention is given over to children who "*shall have the right to such protection and care as is necessary for their well-being*"[4].

b. Jurisprudence on privacy is more comprehensive and detailed than that for child protection in the online space. The laws governing detection tools are inadequate and still evolving because the whole field is in its infancy. The limited number of experts across different subject areas leads to discussions taking place in silos.

c. While there was acknowledgement that CSAM detection tools and grooming detection tools required a different approach, limiting their use to known 'suspects' would make it impossible to deal with the significant volume of 'unknowns' in terms of CSEA content, and the identification of new victims and perpetrators.

d. Each CSEA detection tool is different and has its own objectives. Talking about them as one homogenous group of child safety tools is not helpful - neither is focusing on just one or two. It is important to map and understand the types of application that exist, who is using them and where, and what they can and cannot do. As part of this, it is also crucial to document any evidence that exists on the misuse of these tools, and what measures can and have been taken to address this and mitigate further risk. This will help ensure that decisions regarding the deployment of any individual tool is based on concrete, measurable evidence.

e. Additionally, the lack of clarity on the technical capabilities of detection tools leads to conflicting analogies with cybersecurity tools and broader societal safety technologies. Some of these are about principles and others are more operational. For example, are (content) detection tools comparable to CCTV, or smoke alarms, or anti-malware and anti-virus software? Do anti-grooming tools essentially perform the same function as spam filters? A clearer and more specific evidence-base is needed in relation to individual tools.

f. Because technology is often successful in detecting content, it can offer an easier 'fix' for policymakers than investigation and prosecution, which leads to a situation of dependence on a centralised technology infrastructure and acceptance that content matching technologies are the best and/or primary tool for effective law enforcement. However, it important to note that the technologies under discussion are built for and by private companies to help them detect, remove and report CSEA to law enforcement and hotlines.

g. Discussion about proportionality largely focused on the argument that the more pervasive a technology, the more likely it is that governments and/or technology companies will expand its functions and/or application over time.

h. And while concerns about the 'slippery slope' are always a factor in relation to technology, it is arguable that certain safety and security priorities can be categorised as in the common interest. Furthermore, the potential for tools to be adapted for nefarious purposes is not the same as the ease or likelihood that it will happen.

i. It is undeniable that digital media has been a game-changer both in the perpetration and prevention of CSEA online. CSEA is illegal in most jurisdictions but measuring its prevalence and the effectiveness of the response requires multiple data points and transparent interpretation to enable a comprehensive overview of the issue, whilst always remembering that behind any data are child victims.

4 – https://fra.europa.eu/en/eu-charter/article/24-rights-child#:~:text=Article%2056%20Children%20shall%20enjoy,or%20other%20exploitation%20and%20abuse.

3. Potential solutions

Appropriate oversight is needed to improve transparency and protect against the risk of misuse of automated tools.

a. Some degree of automation is required to cope with the nature, scale and pervasiveness of CSEA online. Tools must be victim-focused, but continued research is needed on what can be done and what works, such as the use of metadata to collect intelligence.

b. Ensuring proportionality requires: 1) safeguards such as strict licensing to counter circumvention and re-engineering; and 2) transparent oversight mechanisms to ensure accountability, for example:
   - Data Privacy Impact Assessments that involve both civil society and governments are already required by the GDPR and have a clear methodology to measure risk and assess the impact of technology on other rights in the broad sense.
   - Technologies deployed in the European Union (EU) should be auditable, and data from reports could be collated controlled in a hash database, potentially based in the EU.
   - A combination of soft and hard regulatory mechanisms is needed to ensure technology innovation can continue, including licensing standards from a responsible research and development perspective.

A culture of transparency and trust must be built.

c. A trustworthy environment is needed to deploy AI tools. Incoming legislation (in the EU and elsewhere) will expose the need for dialogue on fairness, transparency, accountability, safety and privacy.

d. Improved transparency from governments and tech companies can help to alleviate fears about 'mission creep' and misuse of technology, bearing in mind the risk of online services being subverted by users with bad intentions.

Systems not just tools must be strengthened.

e. Law enforcement needs more resources and to work in a smarter way. The conundrum for this debate is that technology has enabled them to do that in many fields not least the field of child sexual exploitation and abuse.

Policymakers need clear and understandable advice.

f. The role of experts is to advise policymakers on the impact of their decisions, which will always be based on certain trade-offs. In relation to tools used to protect children online, they need evidence on the impact of their decision that represent all sides of the debate. Reasons for this include the fact that statistics are often given out of context and can always be used to justify a certain position. There needs to be nuance and context to the numbers. This would help to build trust that is lacking among the key stakeholders in this debate.

Outcomes need to be defined before technology is built.

g. Technology can be designed and/or used for good and for bad. Whether from the perspective of child safety and responsible innovation, or from the perspective of law enforcement, it is necessary to step back, define the desired outcomes, and then design the solutions to meet those.

A differentiated approach to platforms and services.

h. A one-size-fits-all approach to protecting children online may be impractical given the way children engage with technology. If a service is targeted towards children or has a significant user base among children, then implementing a more stringent or different set of safety mechanisms could be explored.

4. Mapping the way forward

It is clear that balancing rights requires sensitivity and expertise. It is not simply a case of balancing privacy with children's right to be protected from sexual abuse; other rights and issues are at play. Child sexual abuse and exploitation online is a growing crime. As the use of technologies such as encryption and artificial intelligence (AI) grow and become more complex, the need to build our collective technical knowledge will increase, as will the need for a more transparent and accountable culture online. It is vital to create a 'coalition of the willing' who are prepared to find compromise and balance but not sacrifice the safety of children.

Following this roundtable, WePROTECT Global Alliance and ECPAT International have identified core ideas that they believe all sides in the debate can coalesce around, and that can help to find a balance between protecting the privacy of all whilst safeguarding children from sexual abuse and exploitation online.

Postscript: On 29 April 2021, the EU reached a provisional agreement in Trilogue to authorise the resumption and continued use of tools to detect CSEA by private companies in the EU. Tools to detect known CSAM, tools to identify potentially new or unseen CSAM, and tools to detect potential grooming fall into the scope of the interim legislation, which has a duration of three years. A number of safeguards were agreed, and the process of developing longer-term legislation has now begun, with draft legislation due to be produced by the European Commission by summer 2021.

a. More safe design and device-level options.

A safety-by-design approach from concept through to design and development could help to alleviate issues later down the line. Device-level options offer an opportunity to intervene early, and to allow more safety and control at user level.

b. Effective implementation of existing legislation and anticipating new legislative proposals.

Increased implementation of legislative instruments that impose duties on EU Member States, such as the 'Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography'[5], should be encouraged. Stronger national legislation can help to push for increased focus on child protection.

The EU can also learn from examples where existing legislation appears to allow reporting to work relatively well, such as in the United States[6]. In addition, new legislative opportunities in the EU should be monitored to ensure a joined-up approach to regulation and policy.

c. Increased mapping and contextualisation of individual tools.

To strengthen policy arguments, a better understanding is needed of how these tools operate and compare with other existing tools, without revealing technical details to potential offenders. This would also help enhance the evidence-base and mitigate fears over the potential risk of 'mission creep' and misuse. One recommendation is to map these tools and identify the parallels and analogies that exist with tools designed to detect, report and remove CSEA online, for example in the field of cybersecurity.

d. Improved knowledge sharing, framing and communication.

It is important to communicate clearly the positive effects of technology in helping law enforcement and government to tackle serious crimes such as human trafficking and child exploitation, and how those tools are designed on the principles of privacy and data protection, and comply with the GDPR. There should be an evidence-based approach to understand the scale, nature and impact of CSEA online. This should integrate input from victims and survivors of abuse and exploitation.

e. Explore a blended options approach.

In other similar policy areas, such as the use of cloud computing, a Code of Conduct has been developed that provides clarity to all stakeholders. This, alongside other possible regulatory options and approaches such as the use of risk management frameworks, improved terms and conditions, licensing and self-regulation, could help to provide a clear set of rules, oversight, and audit process that verifies voluntary compliance.

f. Anticipation of new technology and innovation.

Our use of technology, its evolution and offender behaviour are ever-changing. In order to keep pace, it will be important to anticipate new trends and design any regulation and prevention approaches with changing technology in mind. A situation where the technology precedes the policy leaves ambiguity and risks diminishing trust in the tools that can help to protect children.

5 – https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093

6 – https://www.law.cornell.edu/uscode/text/18/2258A