Council Working Group
on Child Online Protection
Twentieth meeting - From 22 to 23 January 2024

Document CWG-COP-20/INF/12
12 January 2024
English only

Report by South West Grid for Learning (SWGfL)

LEGAL MEASURES RELATED TO CHILD ONLINE PROTECTION

Purpose

Considerations for legal measures related to child online protection - SWGfL perspective.

Action required

This report is transmitted to the Council Working Group on Child Online Protection **for information**.

____

References

https://swgfl.org.uk/

SWGfL contribution to ITU CGW COP

Legal measures related to child online protection

Boris Radanović

12/01/2024

Date: 12/01/2024

Written By
Boris Radanović
boris@swgfl.org.uk
South West Grid for Learning

Contents

Considerations for legal measures related to child online protection – SWGfL perspective

In the digital age, children are increasingly exposed to the digital jungle of the internet, presenting both opportunities and risks. To address the growing concerns surrounding child online protection, **robust, adequate and sensible** legal measures must be implemented globally, with a particular focus on emerging technologies such as end-to-end encryption.

Governments around the world need to recognize the importance of much needed action, today, to safeguard children from online threats, including cyberbullying, explicit content, child sexual abuse and predatory behaviour among other threats such as scams, sextortion and different formats of harmful and illegal content.

Various legal frameworks have been established to address these concerns, emphasizing the responsibility of technology companies, service providers, policy makers, parents and carers, and as well users to create a safer online environment for children. Data Protection and Privacy Laws emphasize the protection of personal data, including that of children. Companies are required to implement measures to ensure the secure processing of children's information. There are obligations on online services that target or collect information from children. Countries worldwide have established national initiatives to combat child exploitation online, often collaborating with international organizations. These initiatives focus on awareness campaigns, reporting mechanisms, and law enforcement cooperation.

Today I want to bring you the discussion point of End-to-End Encryption and its legal impact and challenges.

End-to-end encryption (E2EE) is a technology that secures digital communication so that only the sender and recipient can access the information. While E2EE is essential for privacy and security, it presents challenges for law enforcement agencies and child protection advocates, as it can potentially impede efforts to detect and prevent online threats against children.

Implications for Law Enforcement

E2EE makes it challenging for law enforcement agencies to intercept and monitor potentially harmful communications. Balancing privacy with the need to protect children poses a significant challenge for legislators and technology companies. With E2EE, the ability to detect and report illegal activities, such as child exploitation, may be hindered if better technological solutions are not implemented in its place immediately. Striking a balance between privacy and the duty to report illegal content remains a complex task.

Stricter regulations may require increased cooperation between technology firms and law enforcement agencies.

The legal measures related to child online protection, especially concerning end-to-end encryption, reflect the delicate balance between privacy and the imperative to safeguard children from online threats. As technology continues to evolve, legislators and stakeholders must collaboratively adapt legal frameworks to address emerging challenges while upholding fundamental rights and principles. The ongoing discourse surrounding end-to-end encryption highlights the need for a nuanced approach that ensures both online privacy and child safety are adequately protected.

Hopefully soon, urgently we need to delve into the multifaceted realm of end-to-end encryption (E2EE), a topic of paramount importance in our ever-evolving digital landscape. This technological marvel, designed to preserve the privacy of digital communications, stands as a testament to human ingenuity, offering a sanctuary where individuals can communicate freely and confidentially.

While recognizing the considerable benefits of E2EE, it is essential that we navigate the intricate challenges it poses, particularly in the domain of child protection. Organizations such as the Internet Watch Foundation (IWF), SWGfL and other charities dedicated to shielding children from online exploitation find themselves at a critical juncture.

The vital work carried out by these organizations in identifying, reporting, and eliminating child sexual abuse content involving children is honourable. However, the advent of E2EE introduces a complex dynamic, potentially creating a haven for criminals seeking to exploit encrypted channels for the distribution of CSAM material involving children and hindering the decades of important work of these world leading child safety organisations.

Our shared responsibility, as representatives committed to a safer digital world, is to address these challenges collaboratively. We must find solutions that uphold individual privacy while fortifying the efficacy of child protection efforts. The benefits of E2EE should not be sacrificed but, rather, harnessed and refined to align with our shared vision for a secure, inclusive digital landscape. We must find a way, and we need it now.

In this forum, let us foster an environment of collaboration, encouraging dialogue between technology innovators, policymakers, child protection organizations and others. Through this collective effort, we can craft strategies and frameworks that address the challenges posed by E2EE without compromising the fundamental rights of individuals or the safety of our children.

If the direction of travel is as laid out above, we will not be able to protect the children to the adequate level and we will all fail in one principal duty as adults we all have. Create a better world for all our children.

Parental controls will become ineffective, and our establish routes of protections will disappear, we need change from the ground up, filtering services will become almost obsolete (BYOD will become impossible etc.).

As we navigate the intricacies of our digital age, let us collectively strive for a future where technology serves as a force for good — where innovation and privacy coexist harmoniously with the imperative to protect the most vulnerable among us. Together, we can build a world where every child can explore the online realm without fear, knowing that our collaborative commitment stands strong in ensuring their safety and well-being.

SWGfL strongly supports ITU COP council to discuss setting technical standards for safeguarding children online, for end-to-end encryption or many other emerging technologies we see on the horizon. ITU COP is in a perfect position to create the safe space for discussion and leadership for rational and impactful discussions and interventions. Many of the aforementioned activities, frameworks, legal measures are fragmented and not consolidated in the global space of the internet. There must be a solution to have adequate levels of child protection AND privacy protections for all of us, on global level.

Thank you.