unicef
Office of Research – Innocenti

# Encryption, Privacy and Children's Right to Protection from Harm

Daniel Kardefelt-Winther, Emma Day,
Gabrielle Berman, Sabine K. Witting, and Anjan Bose
on behalf of UNICEF's cross-divisional task force
on child online protection

Office of Research - Innocenti Working Paper
WP-2020-14 | October 2020

## UNICEF OFFICE OF RESEARCH – INNOCENTI

The Office of Research – Innocenti is UNICEF's dedicated research centre. It undertakes research on emerging or current issues to inform the strategic directions, policies and programmes of UNICEF and its partners, shape global debates on child rights and development, and inform the global research and policy agenda for all children, particularly the most vulnerable.

Publications produced by the Office are contributions to a global debate on children and may not necessarily reflect UNICEF policies or approaches. The views expressed are those of the authors.

The Office of Research – Innocenti receives financial support from the Government of Italy, while funding for specific projects is also provided by other governments, international institutions and private sources, including UNICEF National Committees.

For further information and to download or order this and other publications, please visit the website at www.unicef-irc.org.

## INNOCENTI WORKING PAPERS

UNICEF Office of Research Working Papers are intended to disseminate initial research contributions within the programme of work, addressing social, economic and institutional aspects of the realization of the human rights of children.

The findings, interpretations and conclusions expressed in this paper are those of the author and do not necessarily reflect the policies or views of UNICEF.

This paper has been peer reviewed both externally and within UNICEF.

The text has not been edited to official publications standards and UNICEF accepts no responsibility for errors.



For readers wishing to cite this document, we suggest the following form:

Kardefelt-Winther, D., Day, E., Berman, G., Witting, S.K., and Bose, A., on behalf of UNICEF's cross-divisional task force on child online protection (2020). Encryption, Privacy and Children's Right to Protection from Harm. *Innocenti Working Paper 2020-14*. Florence: UNICEF Office of Research – Innocenti.



**Correspondence should be addressed to:**

UNICEF Office of Research – Innocenti
Via degli Alfani 58
50121 Florence, Italy
Tel.: (+39) 055 20330
Fax: (+39) 055 2033 220
florence@unicef.org
www.unicef-irc.org
twitter: @UNICEFInnocenti
facebook.com/UnicefInnocenti

# ENCRYPTION, PRIVACY AND CHILDREN'S RIGHT TO PROTECTION FROM HARM

Daniel Kardefelt-Winther[a], Emma Day[b], Gabrielle Berman[a], Sabine K. Witting[c], and Anjan Bose[d]

(a) UNICEF Office of Research – Innocenti

(b) UNICEF, East Asia and Pacific Regional Office

(c) UNICEF Zimbabwe

(d) UNICEF, Programme Division, Child Protection

**Written on behalf of UNICEF's cross-divisional task force on child online protection**

This working paper provides a short overview of the challenges and opportunities related to child protection and the use of encryption technology. While it does not constitute the UNICEF organizational position on the topic, it is meant to inform UNICEF on the issue and to reach and engage professionals, including non-experts, within and between the child rights and privacy rights sectors.

This paper will provide an overview of the debate around encryption and its possible impact on children's right to protection from harm. It also reflects on the pros and cons of some proposed solutions.

## SUMMARY AND KEY TAKEAWAYS

- End-to-end encryption is necessary to protect the privacy and security of all people using digital communication channels. This includes children, minority groups, dissidents and vulnerable communities. The UN Special Rapporteur on Freedom of Expression has referred to end-to-end encryption as "the most basic building block" for security on digital messaging apps. Encryption is also important for national security.
- End-to-end encryption impedes efforts to monitor and remove child sexual abuse materials and identify offenders attempting to exploit children online. In this way, it also increases the risk of children being re-victimized as materials depicting their abuse continue to be shared online.
- The debate around end-to-end encryption of digital communications has been polarized into absolutist positions. These include advocating 1) for the unlimited use of end-to-end encryption; 2) for the complete abolishment of end-to-end encryption; and 3) that law enforcement should always be able to access encrypted data and will be unable to protect the public unless it can do so. Such polarized positions ignore the complexity and nuance of the debate and act as an impediment to thoughtful policy responses. As noted by the Carnegie Endowment working group on encryption, polarized, absolutist positions in this debate should be rejected.
- Fully understanding encryption in the context of child protection involves a highly complex and technical discussion. To provide a comprehensive picture, extensive consultation and analysis together with external experts is necessary.

## CONTENTS

# 1. INTRODUCTION

In March 2019, Facebook announced the intention to implement end-to-end encryption for its widely used Messenger service, following an industry-wide trend to improve privacy for users of digital communications platforms. The Facebook announcement was welcomed by many privacy and digital rights advocates who see strong encryption as a necessity to guarantee citizen's rights to privacy and freedom of expression.[1]

However, a range of governments and child rights advocates were critical of the Facebook announcement, arguing that it would impede efforts to monitor and remove child sexual abuse materials and identify perpetrators attempting to exploit children. It has been suggested that encrypting digital communications platforms will serve to protect the privacy of criminal offenders, providing them with a safe space in which they can continue to harm children. As a case in point, Apple recently walked back on plans to allow customers to store back-ups of their entire phone in the cloud protected by end-to-end encryption. This was due to objections from the Federal Bureau of Investigation (FBI) of the United States of America (USA), which raised concerns about solving crimes against children.[2]

Children have the same rights as adults, such as the right to privacy and protection of their personal data.[3] Additionally, children enjoy rights tailored towards their specific vulnerability, such as the right to be protected from violence, abuse and exploitation. The use of digital technology brings a new set of challenges to upholding these rights.

UNICEF's new child online protection strategy positions children's right to protection from sexual abuse and exploitation as one of three key objectives. A second objective is to prevent the inappropriate collection, use or sharing of children's data, which is increasingly important to protect children in a digital world. The debate around encryption of digital messaging platforms sits between these two objectives.

Disagreements around platform end-to-end encryption has inadvertently created a perceived conflict between a child's right to privacy and the right to protection from sexual abuse and exploitation. However, the goal of ensuring that children's rights are safeguarded in the digital age involves fulfilment of their rights to both privacy *and* protection from sexual abuse and exploitation. Privacy is often treated as a secondary right. Thus, debates around end-to-end encryption have tended to assume that a safety-maximizing solution (or even a privacy-minimizing solution) is the best way to keep children safe, which is not always the case.

From a rights-based perspective, all human rights and child rights are interdependent, non-hierarchical, and indivisible.[4] A number of international instruments highlight children's rights to protection from sexual exploitation and abuse,[5 6 7] as well as the right to freedom of expression,[8] privacy[9] and access to

1 https://www.wired.com/story/facebook-messenger-end-to-end-encryption-default/

2 https://www.reuters.com/article/us-apple-fbi-icloud-exclusive/exclusive-apple-dropped-plan-for-encrypting-backups-after-fbi-complained-sources-idUSKBN1ZK1CT

3 https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

4 https://www.unicef.org/child-rights-convention/what-are-human-rights

5 Article 34 and 35 of the 1989 UN Convention on the Rights of the Child.

6 Article 3 of the 2002 Optional Protocol to the UN Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.

7 The CRC Committee 2019 Guidelines on the Optional Protocol (CRC/C/156), which specifically reflects on the protocol in relation to a digital world.

8 UN CRC, Article 13

9 UN CRC, Article 16

information.[10] It is important to note that the right to privacy, as with many other human rights, is not absolute and can be limited. However, the limitation of the right to privacy must be *proportionate*, and it is presently unclear what constitutes a proportional response with respect to the implementation of encryption on digital communications platforms. Within this context, this working paper will interrogate some of the challenges that end-to-end encryption poses for the protection of children from sexual exploitation and abuse as well as potential privacy protections that the same technology provides.

## 2. THE BASICS OF ENCRYPTION TECHNOLOGY

In its basic form, encryption is fundamental for any democratic and rights-respecting state to protect its citizens, including children who are increasingly gaining access to digital communications platforms. In simple terms, encryption scrambles communication so that it cannot be read by anyone unless they have the corresponding key to decrypt the data. All IT-systems use a level of encryption to be secure and corporations and states use this to protect against threats to national security such as cyber warfare, data breaches, and interference with elections. Banks use encryption to guarantee the security of financial transactions. Hospitals use it to safeguard personal health information. And, social media companies can use it to protect the personal information and private conversations of their users.

End-to-end encryption is a particularly robust form of encryption where third party intermediaries (such as a service provider) do not have keys to decrypt the communication; it is only readable by the two parties exchanging information. This is distinct from weaker encryption where the company retains a key to decrypt the data on request, either by law enforcement or other organs of government. In this respect, end-to-end encryption is a crucial tool that enables vulnerable groups to communicate and ultimately be able to exercise their right to freedom of expression.

The UN Special Rapporteur on Freedom of Expression has referred to end-to-end encryption as "the most basic building block" for digital security on messaging apps. Because of its critical role, the Special Rapporteur further notes that: "the responsibility to safeguard freedom of expression and privacy may require companies to establish end-to-end encryption as a default setting in their messaging products". And, the Rapporteur also suggests that companies that offer messaging apps "should seek to provide the highest user privacy settings by default".[11]

Without encryption, minorities in some countries may effectively be silenced and put at serious risk of human rights violations and persecution. According to a 2019 report from Freedom House, 71 per cent of the people who use the internet live in countries where individuals have been arrested or imprisoned for content on political, social, or religious issues. And, 65 per cent live in countries where individuals have been attacked or killed for their online activities.[12] Robust encryption therefore touches the core of freedom of expression.

Encryption is also critical to ensure children's safety. Their digital devices and communications contain personal information that could compromise both their privacy and safety if it fell into the wrong hands. This includes data on current and previous locations that might indicate where a child is or will be; what routes they take to school or where they go in their spare time. It is likely to include their

10 UN CRC, Article 17

11 https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf

12 www.freedomonthenet.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf

home address and contact information of people they know, which could be used by a perpetrator to impersonate someone close to the child. Children's digital communications constitute a record of calls, texts, web searches and images, which is private and potentially sensitive information that could be used for threats or blackmail. The application of robust encryption means that this information can be more secure, though it should be noted that the encryption debate is currently centred on content and individual surveillance with less debate regarding encryption of meta-data described above.[13]

An important caveat related to meta-data is that end-to-end encryption primarily addresses violations of the user's privacy by external entities. The company owning the platform is still able to collect meta-data associated with its use even if end-to-end encryption is implemented, which is of considerable monetary value. This means that companies can determine with whom you are communicating, when you are communicating, from where you are communicating and other information about peripheral online activities. Access to this information remains a child rights issue, as it means that children's data can and will be used and shared by companies. While the converse of this is that it may also be used to support development and humanitarian aims of organizations in this field, it is nonetheless a critical child rights concern that is currently not receiving enough attention.

## 3. ENCRYPTION IN THE CONTEXT OF CHILD SEXUAL EXPLOITATION AND ABUSE

Child sexual abuse and exploitation is a major concern worldwide. With access to and use of the internet increasing, child sexual abuse and exploitation is no longer restricted to homes, schools and communities. The use of the internet by perpetrators expands their access to a wider pool of potential victims, as children and adolescents under the age of 18 years constitute an estimated one-third of internet users worldwide.[14] The production, dissemination, possession and accessing of child sexual abuse material is one of the most serious forms of victimization of children in the online space. The internet has also facilitated new forms of sexual abuse, for example made-to-order services that allow the perpetrator to request the production of content in which the age, gender and race of the child are specified according to the perpetrator's sexual preferences.[15] Live-streaming of child sexual abuse is another emerging form of abuse, in which perpetrators can buy access to a stream to observe and direct the abuse of children in real time.[16]

A particularly important consideration for organizations working to prevent the sexual exploitation and abuse of children through the internet is the reporting of child sexual abuse materials from social media companies to the National Center for Missing and Exploited Children (NCMEC) in the USA.[17]

13 Meta-data summarizes information about other data (e.g., numbers of calls made, when, to what number).

14 Livingstone, S., Carr, J. and Byrne, J. (2016). One in Three: Internet Governance and Children's Rights. *Innocenti Discussion Paper No.2016-01,* UNICEF Office of Research, Florence; UNODC (2015). Study on the Effects of New Information Technologies on the Abuse of Children; UNICEF (2017). *The State of the World's Children.*

15 UNODC, Study on the Effects of New Information Technologies on the Abuse of Children, p. 21.

16 *Ibid.,* pp. 22–23.

17 An organization established by act of congress as a national resource center on missing and exploited children. In the USA it acts as the official clearinghouse for reporting of online child sex abuse materials.

The reports made to NCMEC are important for at least two reasons:

1. To ensure that law enforcement is provided with the evidence to investigate individual cases, identify and rescue victims, and prosecute perpetrators;
2. To prevent the re-victimization that occurs when child sexual abuse materials keeps circulating online, as it has severe negative health and social consequences for the victims.

In an open letter to Facebook, Government representatives of the USA, United Kingdom (UK) and Australia[18] warned that implementation of end-to-end encryption on Facebook Messenger would significantly reduce the number of NCMEC reports. This is because, with end-to-end encryption, digital communications shared on Facebook cannot be monitored at scale.

> "In 2018, Facebook made 16.8 million reports to the US National Center for Missing  Exploited Children (NCMEC) – more than 90 per cent of the 18.4 million total reports that year. As well as child abuse imagery, these referrals include more than 8,000 reports related to attempts by offenders to meet children online and groom or entice them into sharing indecent imagery or meeting in real life. The UK National Crime Agency estimates that, last year, NCMEC reporting from Facebook will have resulted in more than 2,500 arrests by UK law enforcement and almost 3,000 children safeguarded in the UK."
>
> "Our understanding is that much of this activity, which is critical to protecting children and fighting terrorism, will no longer be possible if Facebook implements its proposals as planned. NCMEC estimates that 70 per cent of Facebook's reporting – 12 million reports globally – would be lost."

There is no equivocating that child sexual abuse can and is facilitated by the internet and that end-to-end encryption of digital communication platforms appears to have significant drawbacks for the global effort to end the sexual abuse and exploitation of children. This includes making it more difficult to identify, investigate and prosecute such offences. Children have a right to be protected from sexual abuse and exploitation wherever it occurs, including online, and states have a duty to take steps to ensure effective protection and an effective response, including support to recover and justice.

At the same time, end-to-end encryption by default on Facebook Messenger and other digital communication platforms means that every single person, whether child or adult, will be provided with a technological shield against violations of their right to privacy and freedom of expression.

It is critical that we consider how to balance the protection and infringement of these rights when proposing solutions. In this balancing act, it is the different scenarios and their proportional impact in terms of scale and severity that should be in focus. The next sections will therefore interrogate further the consequences of some of the proposed solutions that are currently discussed.

18 https://www.justice.gov/opa/press-release/file/1207081/download

## Impact of end-to-end encryption on law enforcement investigations and content takedown

There is real concern that if digital communications platforms, including messaging apps, default to end-to-end encryption, almost all of the reports provided to NCMEC will cease. This is because it will not be technically possible even for law enforcement to access communications that are end-to-end encrypted, which means that they cannot use software to scan for illegal content. This will limit the evidence available to aid law enforcement investigations. The same applies to automated tools used by the platforms themselves, such as PhotoDNA, to detect known child sexual abuse content. Currently PhotoDNA is the primary tool used to detect child sexual abuse materials on digital communications platforms.

However, there are limitations to the extent to which reports made to NCMEC lead to actual cases of crimes against children being solved. When NCMEC receives cases not involving the US it is referred on to the relevant national law enforcement agency depending on the nationality and location of the child and offender. The response from national law enforcement agencies currently varies widely as a consequence of capacity and resource constraints. Even though it is hoped that this will change in the future with many countries upscaling their national response systems, including with UNICEF support, it remains a reality that capacity and resources to combat these crimes are extremely limited in many contexts. This means that a sustained stream of NCMEC reports will not necessarily lead to a safer environment for children until national law enforcement agencies are allocated sufficient resources to arrest and prosecute child sexual abuse offenders, including those operating in the digital environment. This is an area where UNICEF could use the data currently being shared by Facebook with NCMEC to advocate for more resources to national law enforcement agencies and INTERPOL. However, it is currently unclear how many investigations or arrests directly derive from NCMEC reports at the global level, or how many fewer would have been made with end-to-end encryption implemented. Attempts at collecting this data is currently underway by INTERPOL, but the lack of information makes it difficult to assess the potential drawbacks of implementing end-to-end encryption on Facebook Messenger specifically. The loss of reports to NCMEC has been one of the key arguments against implementing end-to-end encryption, but until more data is available, it is not possible to determine what implications this will actually have on law enforcement operations.

Nonetheless, it must be highlighted that national law enforcement agencies have only been receiving data from NCMEC for a few years. This data is vital to enabling nations to understand the extent of the problem of child sexual abuse materials online and how it is accessed or shared by its citizens, even if it is only reported from a few platforms. In the absence of other data related to child sexual abuse materials shared online, if the NCMEC data disappears then it may be more difficult to make the case for increased government investment in tackling child sexual exploitation and abuse. Or even to argue for increased efforts by industry to make their platforms safe.

When it comes to preventing re-victimization, by removing child sexual abuse materials in circulation, end-to-end encryption of digital communications platforms as currently implemented will make this more difficult. Further, law enforcement will unable to intercept messages of suspected offenders in the way they would have been able with unencrypted messages or phone calls. These are serious drawbacks and UNICEF with its partners in the technology sector should consider how to mitigate these as end-to-end encryption becomes more common.

Even if some platforms remain unprotected by end-to-end encryption, it is likely that perpetrators who understand the technology are already using other means of communication. Popular messaging services such as WhatsApp (owned by Facebook), Telegram and Signal are all using end-to-end encryption and

may therefore host a higher number of offenders who will remain untraceable. It can be argued that in the context of Facebook Messenger specifically, it is better to be able to intercept crimes against children perpetrated via one popular digital communications platform than none at all. But, equally, privacy and security implications and potential for commercial exploitation follow for *all* users of a digital communications platform if it remains unprotected by end-to-end encryption. While the impacts of such privacy infringement may be limited for many people, longer-term or emerging impacts are at this point difficult to predict.

## Solutions to balance privacy rights and protection from sexual exploitation and abuse

The perceived conflict between rights to privacy and data protection on the one hand and protection from sexual exploitation and abuse on the other creates the impression that these two rights are competing. However, several solutions, both technological and legal, have been put forward to attempt a proportionate balancing act. Some of the pros and cons of these will be discussed in the next sections.

### *Exceptional access for law enforcement*

One of the significant concerns in relation to privacy is the proposed solution that technology platforms should provide exceptional access ('backdoors') for law enforcement to access and seize personal information through a search warrant. This would make law enforcement responses more similar to other forms of crime offline, when there is substantial evidence of a crime being committed. This would avoid turning certain online spaces into an impenetrable fortress where law enforcement cannot conduct investigations, which is currently the case for applications such as WhatsApp, Signal and Telegram. However, the exceptional access solution is challenging from a technological perspective. Developing a system that allows law enforcement exceptional access always makes the system vulnerable to unauthorized access by (malicious) third parties, including foreign governments, even if intended solely for specific government access. Further, governments themselves may also abuse this power. The extent to which governments may abuse it varies depending on the regime. Some commentators have stated that even in countries that are generally assumed to enjoy a strong rule of law, history has proven that whenever government agencies gain access to personal data, that data is certain to be leaked elsewhere.[19] There is also serious concern that once exceptional access solutions are put in place, the boundaries for when these can be employed might shift over time and come to include a greater number of offenses, justified by vague premises and diminished oversight, all of which will be largely invisible to the public.

As an example of exceptional access solutions, in July 2019, the 'Five Eyes' security alliance comprised of the UK, US, Canada, Australia and New Zealand, called on tech firms to allow law enforcement agencies access to encrypted materials.[20] In an open letter to Mark Zuckerberg in December 2019, the UK Home Office called for the use of the CLOUD Act to develop international agreements for information sharing by tech companies with and amongst selected democratic countries.[21] In response, an open letter to Mark Zuckerberg was sent by the Center for Democracy & Digital Technology together with more than 100 civil society organizations including Human Rights Watch, Article 19, and Privacy International. That letter called on Facebook to resist calls to create exceptional access for law enforcement to users' messages as this would fundamentally weaken the privacy and security of all users.[22]

19 https://hbr.org/2016/05/the-downside-of-the-fccs-new-internet-privacy-rules

20 https://www.reuters.com/article/us-security-fiveeyes-britain-idUSKCN1UP199

21 https://www.gov.uk/government/publications/open-letter-to-mark-zuckerberg/written-testimony-of-chloe-squires-director-national-security-home-office

22 https://cdt.org/insights/open-letter-facebooks-end-to-end-encryption-plans/

As noted by Freedom House, the mere access to social media by governments across the globe has already had a chilling effect on human rights.

> "While social media have at times served as a level playing field for civic discussion, they are now tilting dangerously toward illiberalism, exposing citizens to an unprecedented crackdown on their fundamental freedoms. Moreover, a startling variety of governments are deploying advanced tools to identify and monitor users on an immense scale." [23]

As it stands, there is no agreement on whether exceptional access is a viable solution. Furthermore, exceptional access would still only allow law enforcement to target known or suspected offenders, but it would not allow technological solutions such as Microsoft PhotoDNA in its current form to function on an encrypted service. This is because PhotoDNA relies upon scanning every image that passes through a digital communications platform, assigning each image a unique hash, and then checking these hashes against the NCMEC database of illegal images. To deploy PhotoDNA through an exceptional access solution, law enforcement would have to access and scan all messages on a platform, which would amount to mass public surveillance rather than exceptional access.[24]

One of the creators of PhotoDNA asserts that due to recent advances in encryption and robust hashing technology it would be possible to adapt PhotoDNA for use within an end-to-end encrypted system.[25] This would enable images to be analysed against the database of hashes maintained by NCMEC without the need for decryption. It is not clear whether this proposal solves the privacy concerns from a technical point of view, but it seems an important angle that UNICEF could pursue further with partners in the technology sector.

***Client-side scanning of images***

An alternative option to the exceptional access solution is client-side scanning of images. Client-side scanning means that any outgoing communication flow from a personal device, whether using an encrypted communication system or not, is checked against a hash list of known child sexual abuse images. If there is a match, either the system refuses to send the message, reports the attempt to law enforcement or NCMEC, or a combination of these responses. This solution is portrayed as more data protection friendly compared to exceptional access, as it still upholds end-to-end encryption and its data protection benefits by filtering the communication at the level of the transmitting device.

However, this approach risks providing a blueprint for mass surveillance, as it may not be possible for the user or civil society to monitor the hash list used by their phone to ensure that it was only reporting or preventing the transmission of child sexual abuse images. Hashes for other sensitive but legal content (such as political or sexual) could be added to the database and without the user's knowledge.[26] Furthermore, it deteriorates the purpose of end-to-end encryption relating to freedom of information and expression, as the content of the communication is filtered by default. But despite its limitations in relation to privacy and security, it has been suggested that end-point scanning of images would probably do more to systematically address child sexual abuse materials online compared to providing exceptional access to law enforcement.[27]

23 https://www.freedomonthenet.org/report/freedom-on-the-net/2019/the-crisis-of-social-media

24 https://www.lawfareblog.com/encryption-and-combating-child-exploitation-imagery

25 https://www.ischool.berkeley.edu/news/2019/opinion-facebooks-plan-end-end-encryption-sacrifices-lot-security-just-little-bit-privacy

26 https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption

27 https://www.lawfareblog.com/encryption-and-combating-child-exploitation-imagery

***Compelled disclosure***

Another solution discussed is compelled disclosure.[28] Compelled disclosure means that the legal framework authorizes law enforcement to force a suspect to either hand over their keys to the encrypted system or provide law enforcement with plain text data from their device. This solution has the advantage that no general vulnerability is created within the system, while still allowing police to target suspects and retrieve the information they require. However, the compelled disclosure solution also has disadvantages: it requires an identified suspect and formal processes like the legal issuance of a search warrant; and it cannot decrypt data intercepted in real time and must be carefully balanced against fair trial principles such as the right against self-incrimination. It can also compromise the right to privacy as personal information not pertinent to the crime under investigation may be revealed. This is also a reactive rather than a proactive response and requires a suspect before the illegal materials can be found, which would still preclude the use of tools that can remove child sexual abuse materials systematically at scale.

## 4. CONCLUDING REMARKS

Human rights organizations need to adopt a nuanced position on encryption and possible technological and legal solutions to ensure that children's right to protection in all its forms is respected. Without a nuanced position, there is a risk of inadvertently supporting the dilution of the rule of law and implementing solutions that compromise children's safety.

Solutions that seek to weaken or halt access to strong encryption are currently being pursued by some States as a means to protect children, but these have come under recent criticism from the UN Special Rapporteur on the right to privacy as a "well-intentioned but fatally-flawed" approach.[29] As human rights organizations we need to see the whole picture and ensure that all child rights implications of our proposed actions are given due weight, and not only those that apply to one part of child protection.

Additionally, the debate around end-to-end encryption intersects with debates around the accountability of digital communications platforms. Up until now, platforms based in the USA have enjoyed freedom from liability for content posted on their sites under section 230 of the Communications Decency Act.[30] However, there is a bill currently before the USA Congress, the EARN IT Act, which if passed would impose liability for platforms who 'knowingly' host content that is harmful to children.[31] If Facebook encrypts all of the content on their apps, then they cannot 'know' that their platforms are in any way harming children, or take steps to find out, such as through the use of image scanning software, or moderation techniques. Companies may therefore have multiple motives for their encryption proposals; some promote privacy and others protection from liability. The debate around end-to-end encryption therefore intersects with another highly polarized debate, the enactment of the EARN IT Act, which has broad support from the child rights sector and broad opposition from the privacy rights sector.

28 https://en.wikipedia.org/wiki/Key_disclosure_law

29 Human Rights Council (2020), *Report of the Special Rapporteur on the right to privacy,* Firty-third session, 24 February – 20 March 2020. A/HRC/43/52

30 https://en.wikipedia.org/wiki/Section_230_of_the_Communications_Decency_Act

31 https://www.cnet.com/news/why-your-privacy-could-be-threatened-by-a-bill-to-protect-children/

In the end, we need to appreciate that the right to protection includes ensuring privacy and security. We need to look to new technologies and new approaches to tackle sexual exploitation of children in all of the spaces they inhabit. This will likely involve bringing together technologists, privacy experts, law enforcement and child protection specialists for some challenging conversations, that will allow competing interests to truly be understood and balanced. At the same time, our focus on technology cannot overshadow primary prevention as a means to ensure no child is initially victimized, which requires continued work by UNICEF and its partners to strengthen its national child protection systems.

Although frequently mentioned in the debate, it is incorrect to suggest that children will have their rights better respected if digital communications platforms remain unencrypted; this is the case regarding some risks, but not all. The debate also needs to consider severity and scale of impact. Certainly, violations of a child's right to protection from sexual abuse and exploitation have severe and often lifelong consequences. For some, the consequences of privacy, security and data protection risks can also be severe, long-term. And a key consideration is that those risks will affect *all* users of digital communications platforms; every child and every adult in the world, now and possibly for the future, and the consequences are difficult to predict. There is a need to explicitly consider how protection and privacy can be most effectively ensured in conjunction and think through the potential implications of our proposed solutions – legally, globally, technologically and for the future of our democratic principles and the rule of law.

In the interim, we suggest following the recommendations from the Carnegie Endowment working group on encryption,[32] and make clear that an absolutist position for or against encryption and access to encrypted data act as impediments to thoughtful policy responses. To provide a comprehensive picture, extensive consultation and analysis together with external experts is necessary.

32 https://carnegieendowment.org/files/Encryption_Policy-Key_Takeaways.pdf

unicef
Office of Research-Innocenti