Privacy *and* Protection:

A children's rights approach to encryption

CRIN CHILD RIGHTS INTERNATIONAL NETWORK

defend|digital|me

Acknowledgements

We would like to thank all of the interviewees and questionnaire respondents who took part in the research for this report as well as everyone who reviewed or provided comments on drafts.

CRIN is a creative think tank that produces new and dynamic perspectives on human rights issues, with a focus on children's rights. We press for rights - not charity - and campaign for a genuine shift in how governments and societies view and treat children.

defenddigitalme is a call to action to protect children's right to privacy. We are teachers and parents who campaign for safe, fair and transparent data in education, in England and beyond | defenddigitalme.org

Illustrations by Miriam Sugranyes.

First published in January 2023.

The Child Rights International Network (CRIN) is registered in the United Kingdom and regulated by Companies House and the Charity Commission (Company Limited by Guarantee No. 6653398 and Charity No. 1125925).

defenddigitalme group (defenddigitalme) is registered in the United Kingdom at Companies House (Company Limited by Guarantee No. 11831192).

Citation: Privacy and Protection: A children's rights approach to encryption. (2023) Child Rights International Network and defenddigitalme.

Contents

Executive summary

The debate on encryption and children's rights is often framed as a divide between a child protection approach and a civil liberties focus. But this polarisation masks a more complex truth.

Children, the rights and their interests are on all sides of this discourse. Applications of encryption can protect or expose children to violence, promote or undermine their privacy, encourage or chill their expression. Encryption engages nearly all of their human rights from a wide variety of angles.

We are at a point in how the digital space is controlled, accessed and regulated that will shape how children engage with it for decades to come. It is essential that such policy-making is based on an informed understanding and respect for its impact on the full range of their rights and meaningfully includes everyone whose rights are at stake. The report aims to explore the issue of encryption in its full complexity and to set out a principled approach to the issue built on those rights.

The history of encryption

Encryption and the debates around its use have a long history. To understand the challenges that exist today, the report begins by providing a brief overview of this history, from the beginning of the "crypto-wars" in the 1970s with the classification of encryption as munition under US law, to the emergence of computers in commercial companies in the 1980s, and the growing use of personal computers and the World Wide Web in the 1990s. The report presents the attempts to obtain keys giving "back door" access to communications, such as the Clipper Chip initiative, the hacking of smart-card companies and government pressures on encrypted webmail services. It also looks into the more recent proposal from agencies to add a silent participant to online chats and calls, and objections to it. Against this background, the report examines the various policy drivers of the push to restrict encryption over time, from counter-terrorism and the fight against crime, bribery and corruption, to dealing with misinformation and mob violence, and the current focus on online child sexual abuse.

Understanding the technology

Developing a children's rights approach to encryption requires a thorough understanding of the technology: how it works, how it is used and how it is integrated into the digital environment.

The report explores the place of encryption in the digital environment, analysing the various technological tools with regard to their uses, benefits and compromises. It starts with a basic explanation of how the Internet works and how the World Wide Web runs on it. It then delves into how encryption helps create secure websites, and shows how the shift to greater security of websites creates challenges for organisations responsible for creating lists of websites to be blocked or monitored. It also discusses the difference between content and metadata, and the powerful uses of metadata, especially when it is aggregated and analysed. It explores the argument that metadata can indicate patterns that suggest illegal activities, including the idea that metadata should be used to identify and justify targeted interventions to address online child sexual abuse.

Beyond confidentiality, the report highlights other uses of encryption, such as anonymity and authentication, drawing on the argument that encryption is not a single technology, but is more akin to a concept. It then emphasises the impact of encryption on children's lives in a variety of spheres, from health to education and play, and discusses the issues thrown up by parental monitoring or control services.

Against this background, the report then details specific technologies that are relevant to the debate on encryption and children's rights, particularly those used to identify and remove child sexual abuse material. It examines the scanning of unencrypted content to match known images through the example of PhotoDNA and addresses the expansion of this method beyond the identification of child sexual abuse images into the area of counter-terrorism. It also highlights the dearth of information on similar technologies that would be able to operate in live and real-time digital environments. The report then analyses the difficulties of identifying illegal behaviour in encrypted environments. It focuses on client-side scanning - a method of analysing content on device - and discusses experts' different takes on it, from its perceived advantage as a less intrusive means of identifying content by comparison with having access to the entirety of the user's communications, to the criticism that it creates security challenges, breaks the user's expectation of privacy and that it could be repurposed for surveillance and censorship.

The report then discusses homomorphic encryption - a technology which permits computations on encrypted data without decrypting it - and other emerging technologies. It shows how some view these privacy-enhancing methods as a way to move the debate forward, while others underline that these technologies are not yet fully developed, that developing them is very expensive, and that they still present security, privacy and jurisdictional problems. The report then addresses covert access to live content via wiretapping - adding a silent party to encrypted communications, or exploiting security vulnerabilities through "legal hacking". It discusses the extent to which these methods should be acceptable and subjected to safeguards, as well as the warning that this could lead to a constant "cat-and-mouse game" of fixing a vulnerability exploited by bad actors as well, and then having to create a new one. The report then notes the possibility of obtaining covert access to live content through malware and interception, for example with software like "Pegasus". The explanations around technology conclude with the argument that encryption can be broken in principle, if not in practice, if its aims are compromised. The report also discusses user reporting and finds that it can be implemented without posing risks to privacy and security in encrypted environments, though user reports need adequate and timely responses from platforms.

Frictions and faultlines: The search for consensus

The encryption debate was once described as "thermonuclear", with "emotions running high on either side". To move beyond the divides that currently exist with regard to encryption, it is necessary to understand the frictions, fractures and faultlines that exist in this space as well as where there is room for consensus.

The report explores the diverse perspectives adopted in current discussions. These perspectives are drawn from the literature review, as well as interviews, questionnaires and conversations with the full range of organisations and experts working in this space, including child protection, children's rights, digital rights, privacy and data protection, Internet regulation and technology industry.

The report explores several themes, mapping areas of agreement and disagreement to understand the debate and help move the conversation forward. The report finds a number of areas of consensus, including a fundamental agreement that online child sexual abuse and exploitation requires urgent action. Where interviewees disagreed is how best to achieve this goal while protecting human rights. A wide range of experts described the highly emotional nature of the debate, which risks preventing engagement across different areas of expertise, though some felt that some progress is being made. Another difficulty is the overreliance on specific numbers regarding the scale of online child sexual abuse. Participants from different sides of the spectrum argued, for different reasons, that these numbers are not a true reflection of the nature and extent of the problem. On the one hand, child sexual abuse offences are underreported. This is a particular problem in light of the emerging trend of sextortion, a combination of white collar crime and child sexual exploitation, because digital payment platforms do not report financial activity as sexual abuse. On the other hand, reports contain duplicate pieces of content and images shared consensually between teenagers. Most importantly, it is far from clear to what extent reports of online child sexual abuse material lead to investigations and arrests of offenders and the safeguarding of children.

Interviewees also agreed that online regulation should not be treated as a matter of "privacy versus protection", or "the privacy of adults versus the protection of children", but that there should be a balanced conversation about all of the human rights involved. Some children's rights advocates saw the current polarisation as a general failing in the discourse around children, which views them as "objects of protection instead of fully formed subjects of rights". They also argued for a better understanding of how privacy impacts children's development. Many participants emphasised that privacy enables the exercise of other rights, including protection from violence. But some warned that the encryption should not be seen as wholly beneficial to protecting privacy, since the privacy of those who have been sexually abused receives insufficient attention.

A related concern was that not enough emphasis is put on safety. Several interviewees drew attention to examples of victim-blaming, particularly in the casual use of language. There is a clear consensus that survivors of child sexual abuse must be meaningfully included in reform processes, but no assumption should be made about their views, as they are a diverse group with varied experiences and perspectives.

There was also agreement among interviewees that technology is a central topic in addressing the issue of online child sexual abuse. While some argued that technology both directly and indirectly facilitates abuse and therefore technical solutions should be developed, others cautioned against "techno-solutionism". They emphasised that different policy options, some of a technological nature and others not, can be used to achieve different outcomes. Therefore the starting point should be the goal to be attained, rather than the merits of any particular technology.

The question of who has a legitimate role to play in deploying technology was also a common theme in interviews. Some participants suggested using the existing technologically-based investigative powers of law enforcement authorities - though an objection was raised that the scale of abuse presents a challenge. Others questioned whether law enforcement should rely on the "stranger danger" narrative to use automated tools at scale. Yet others went further and warned that, due to insufficient investment, the capacity of law enforcement to address online child sexual abuse has deteriorated. Some also warned against mission creep for law enforcement. This was a particular concern regarding children from disadvantaged and marginalised communities, who are more likely to have negative experiences of policing.

In light of these limitations of technology and who should use it, some interviewees called for a systems approach to online child sexual abuse. As technological steps they suggested cumulative small adjustments regarding system design and the design of services. More broadly, they argued it is necessary, though perhaps less politically convenient, to focus on the other actors in the wider ecosystem instead of looking for the technological silver bullet. They called for more investment into schools and education, health services and social services - especially those helping survivors in their recovery.

There was general agreement on the need for democratic oversight in the form of platform regulation. Interviewees argued in favour of more consistency and accountability, with clear guidance on what is expected of companies and how they should proceed. However, participants diverged on where to place the burden for action. Some saw the tools that platforms create as benefiting law enforcement, while others warned against a dependence on "monopolistic tools" built by "politically unaccountable actors" and the privatisation of law enforcement functions.

Many interviewees observed that the debate is Anglo- and Euro-centric, and emphasised that laws cannot be simply transplanted from one jurisdiction to another, but must be tailored to the national context. For example, some highlighted specific challenges faced outside Europe and North America, such as design discrimination and the use of low-end devices.

The impact of encryption on children's rights

The report applies a children's rights approach to the rich and complex perspectives identified. It treats the UN Convention on the Rights of the Child as the agreed international framework that covers the full range of children's rights, and analyses the benefits and risks that the applications of encryption can pose to Convention rights. It discards the "privacy versus protection" opposition, showing that it is not the case that encryption poses only benefits for privacy and only risks for the protection of children.

Encrypted channels can be used to circulate child sexual abuse material, which violates the privacy of victims. At the same time, encrypted channels can be used to communicate safely with the outside world and seek help where children are victims of violence, for example perpetrated by a family member. Moreover, encryption engages not only children's rights to privacy and protection from violence, but also non-discrimination, the right to life, freedom of thought, conscience and religion, the right to health, and even the protection of children affected by armed conflict. The report looks into more detail at the right to privacy and its permissible restrictions as an example for how to engage with regulation and the tensions in the application of children's rights.

Moving beyond "privacy versus protection", the report explores how the impact of encryption varies depending on children's backgrounds, needs and identities - especially where they belong to disadvantaged or marginalised groups. The scenarios aim to emphasise children's agency in exercising their rights in a wide range of settings.

In relation to the State, the report examines the role of encryption for children who are politically active but live under repressive regimes, children whistleblowers and activists, as well as for children who want to make decisions about their own body (for example, regarding abortion), and those whose rights are restricted under general human rights law (for instance, under states of emergency or for the protection of national security). In relation to the family, the report looks at the impact of encryption for children whose interests or views are different from those of their parents, and children who might be put at a disadvantage because of their parents' status. In relation to businesses, the scenarios focus on the disproportionate impact that platforms can have on children's rights, particularly where platforms are extremely influential or collect children's metadata.

Legislative proposals

In recent years, there has been an increase in the number of proposals for legislation and other initiatives around the digital environment which impact encryption, often with the aim of keeping people safe.

The report provides a brief overview of three of these proposals that were put forward in the US (the EARN IT Act of 2022), the UK (the Online Safety Bill) and the EU (the proposal for a Regulation laying down rules to prevent and combat child sexual abuse). Their aim of protecting children online, particularly from sexual abuse and exploitation, is uncontroversial. However, the report sets out important areas of disagreement regarding the impact of these proposals for encryption and children's rights.

A children's rights approach to encryption: Principles for policy makers

The realisation of the full range of children's rights in digital environments is complex and nuanced. There are no one-size-fits-all solutions. The report sets out a principles-based set of recommendations for future regulation in ways that respect children's rights.

The report puts forward ten principles for a children's rights approach to encryption. Both the framing of the issue and the ultimate policy outcome are important, so the first five principles deal with questions of process, while the latter five concern the substance of policy-making.

Process

1. **Actions affecting the digital environment must respect the full range of children's rights, from protection from violence to privacy and freedom of expression.**
   - Discussions need to move beyond the polarisation "privacy versus protection" and recognise that all children's rights are equally important and support each other.
   - All interventions that have a significant impact on children must be based on child rights impact assessments.

2. **No single law, policy or technology can protect children online or secure their human rights more broadly. Interventions engaging encryption must be seen within a wider ecosystem with many actors.**
   - Encryption should not be the starting point in policy discussions. Policy-makers should instead first identify the goals to be achieved and then consider a range of solutions, technological or not, taking into account the variety of actors involved in the societal ecosystem
   - Stakeholders should be wary of one-size-fits-all technological fixes.
   - The complete child protection system, from law enforcement and the justice system, to social services and victim recovery, should be supported.

3. **All those with relevant expertise (e.g. in child protection, technology and Internet regulation, data protection and privacy, general human rights etc.) must be involved in discussions and decision-making regarding children and the digital environment, including on encryption.**
   - Special attention should be paid to the framing and language used.
   - There should be more emphasis on the importance of accurate data.

4. **Children and other directly affected communities, for example survivors of child sexual abuse or those disproportionately affected by intrusive data practices, must be heard and their views given due weight.**

5. **The digital environment is interconnected and regulation in one jurisdiction is very likely to cause ripple effects in others, therefore policy-makers engaging with encryption must address the impact beyond their own jurisdiction.**

Substance

6. **There should be no generalised ban on encryption for children.**

7. **Interventions engaging encryption must consider and address specific political, economic, social and cultural contexts.**
   - Participants to the debate should promote a better understanding of the wide range of uses of the digital environment, particularly beyond the Anglo- and Euro-centric contexts.
   - Stakeholders should recognise that technology can be repurposed to further a variety of policy goals, including surveillance and the identification of legitimate material.

8. **Restrictions on qualified children's rights such as privacy must be necessary and proportionate. They should be sufficiently clear and precise, limited to achieving a legitimate goal and the least intrusive way of doing so.**

9. **Policy-making should address the role of business.**
   - Where businesses obtain knowledge of illegal content on their services, they should promptly report this to authorities.
   - Companies should publish transparency reports regarding how they prevent and remedy violations of children's rights on their services.

10. **Children must have access to justice for all violations of their full range of rights in the digital environment, including where encryption is engaged. Free, effective and child-friendly complaint mechanisms, alongside independent oversight mechanisms, should be available.**
    - Confidential, safe and child-friendly user reporting should be made available, and "trusted flagger" mechanisms should be considered.
    - Inadvertent outcomes due to error from automated processes must be reversible through human support.

Introduction

Encryption is everywhere. When you browse a secure website, communicate through a messaging app, access online banking, or entrust your data to an online health service, you are relying on encryption. For children, as for adults, encryption is a part of their lives, keeping their personal information and communications safe, online and offline.

The debate on encryption and children's rights is often framed as a divide between a child protection approach and a civil liberties focus. But this polarisation masks a more complex truth.

Children, their rights and their interests are on all sides of this discourse. Applications of encryption can protect or expose children to violence, promote or undermine their privacy, encourage or chill their expression. Encryption engages nearly all of their human rights from a wide variety of angles.

The impact that encryption has, whether positive or negative, can also vary significantly for children depending on their backgrounds, needs and identities. If the approach to encryption is to take all children's rights seriously, it must engage with how children are affected globally, including the specific experiences of children from disadvantaged and marginalised communities.

Towards a children's rights approach to encryption

This report aims to recognise the full complexity of how encryption affects children and to set out an approach that is based on the full spectrum of their rights.

The development of encryption is intertwined with the technological developments of the late 20th century and the Internet specifically. If we are to understand where we are now, we must see how we got here. With this in mind the report starts with the history of the debate around encryption, from the "crypto-wars" since the 1970s to the challenges we face today.

Responding to the need for an accessible analysis of the relevant technology, the report then examines what encryption is and how it works. This includes a discussion of technology used to identify child sexual abuse material online as well as online sexual exploitation and abuse. We aim to be clear about the benefits, costs and compromises of this technology, so that its legitimate role can be assessed.

If we are to move beyond the divides that are currently present in this field, we must understand the frictions and faultlines that exist in this space as well as where there is space for consensus. Interviews with the full range of organisations and experts with a stake in this issue were at the heart of the research. The

report represents and examines the range of perspectives and approaches of those working on issues related to encryption, in order to help move beyond the polarisation that has been so present in the debate around encryption.

Building on this foundation, we explore how encryption engages with the full range of children's rights, treating the UN Convention on the Rights of the Child as an agreed international framework and examining how it applies to children affected by, or who use, technology that involves encryption. This analysis engages with the tensions that can exist between the desire to protect children from violence as well as to protect their privacy and the privacy of the public at large, but finds that we must move beyond a privacy versus protection framing if we are to ensure that all children's rights are protected in this context.

Shaping the online space for children for the decades to come

Ultimately, with this report we present our perspective on the issue and set out principles for a children's rights approach to encryption. The aim is to provide a basis to shape how to design and evaluate policy-making on this issue grounded in the full range of children's rights.

We are at a point in how the digital space is controlled, accessed and regulated that will shape how children engage with it for decades to come. It is essential that such policy-making is based on an informed understanding and respect for its impact on the full range of their rights and meaningfully includes everyone whose rights are at stake.

Methodology

This research focused on the impact of encryption on children's rights, particularly in the context of the current debate around encryption and online child sexual exploitation and abuse. The report draws on a literature review, as well as semi-structured interviews and background conversations with experts working on this topic, and written answers provided in response to a questionnaire.

The literature review targeted particular areas of agreement and disagreement among the participants to the debate, and sources were identified through desk-based research and recommendations from professionals working in this space. The literature review informed some of the report's analysis, and was also used to structure the approach to interviews. Interviewees were drawn from a range of spheres, including child protection, children's rights, digital rights, privacy and data protection, Internet regulation and technology industry.

Adult survivors of online child sexual exploitation and abuse also took part in interviews. In order to take into account children's views on this issue, reference was made to literature which cites studies carried out by researchers working directly with children.

In addition to semi-structured interviews, the report draws on background conversations, which were in most cases unstructured. Questionnaires were sent to a variety of organisations and covered similar questions to those in the interviews. With questionnaires, the intention was to reach organisations outside the dominant Anglo- and Euro-centric spaces, and give them the opportunity to provide input in a flexible format. Where participants agreed, individual views are directly attributed to them in order to improve the transparency of the debate, convey its richness and help map a way forward.

We would like to thank all of the interviewees and questionnaire respondents who gave us their time to take part in the research for this report as well as everyone named and anonymous, who reviewed or provided comments on drafts.

Speaking, sharing and hearing words of mutual recognition is an important step in creating collaborative, accountable, continuous, and respectful relationships across communities who inhabit different territories in the shared landscape of this debate.

The authors are indebted to the open and supportive nature of the wide range of contributing comments from individuals and organisations we were given, in particular those experienced in child sexual abuse and violence against children, and those working in support of victims and survivors, as well as experts in cryptography, in policy, from institutions, civil society, academia and from industry.

We have done our best to accurately represent others' views, but the report and any errors outside direct quotes are ultimately the opinion and responsibility of the authors.

Public list of interviewees

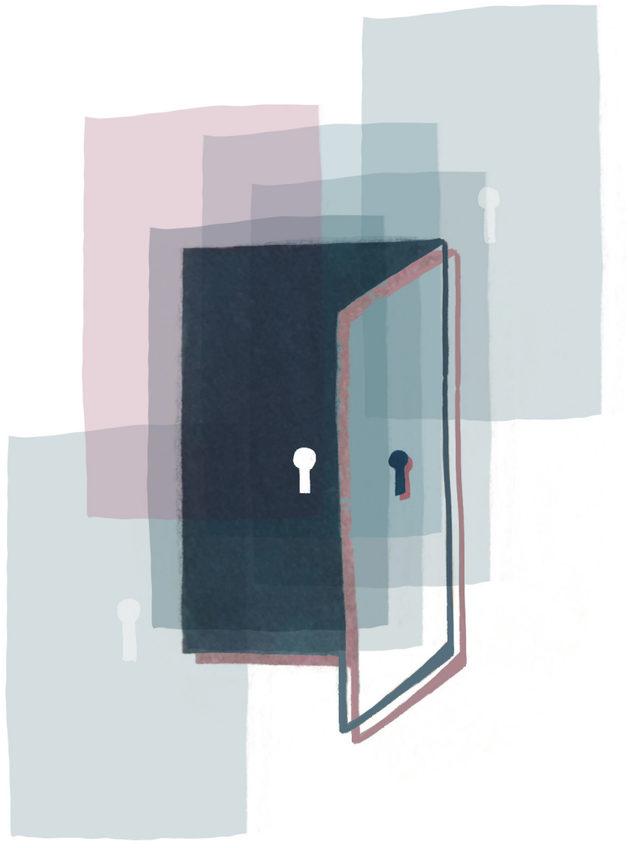
	Representative	Organisation
1.	Duncan McCann and Izzy Wick	5Rights Foundation
2.	Maria Góes de Mello, and João Francisco de Aguiar Coelho	Alana Institute (Instituto Alana)
3.	Iverna McGowan Smyth	Centre for Democracy and Technology (Europe Office)
4.	A representative	Coram International - Coram Children's Legal Centre
5.	Amy Crocker and Isaline Wittorski	ECPAT
6.	Joe Mullin	Electronic Frontier Foundation (EFF)
7.	Tom Fredrik Blenning	Electronic Frontier Norway
8.	Ella Jakubowska	European Digital Rights (EDRi)
9.	Hosein Badran	Internet Society (ISOC)
10.	Daniel Sexton and Michael Tunks	Internet Watch Foundation (IWF)
11.	Rhiannon-Faye McDonald and Victoria Green	Marie Collins Foundation
12.	Gail Kent and Helen Charles	Meta
13.	Yiota Souras and Jennifer Newman	National Center for Missing & Exploited Children (NCMEC)
14.	Dianne Ludlow	One in Four
15.	Caroline Wilson Palow	Privacy International
16.	Chloe Setter	WeProtect Global Alliance
17.	Ian Brown	In a personal capacity
18.	Wendy M. Grossman	In a personal capacity
19.	Richard Wingfield	In a personal capacity

We are also grateful to representatives from the following organisations, who provided written answers in response to our questionnaire:

- Africa Media and Information Technology Initiative (AfriMITI)
- Alexander von Humboldt Institute for Internet and Society
- Bits of Freedom
- Data Privacy Brazil Research Association.

We also thank other participants working in this space who provided input during approximately 15 hours of private conversations.

We extended invitations to other stakeholders working in the sector including law enforcement and the charity sector. We hope to be able to engage with those who were not able to take part in this research in the future.



Encryption: A brief history

Encryption is not new, nor are the disputes around how it should be used and regulated. Public policy discussions around the use of encryption now commonly focus on the challenges it poses to identifying and preventing online sexual exploitation and abuse of children, but this is the latest development in a long-running debate. Understanding the history of encryption is essential in order to understand the tensions and disagreements that exist today.

The history

State desires to control cryptography - the techniques for secure communication in the presence of unintended recipients - have a long history. Among the best known state systems and attempts to break those of the other side, were those used during World War II to enable and decipher state secrets between one another, using knowledge of what the other side was planning in information warfare.

After World War II, the United States (US), United Kingdom (UK), Australia, Canada and New Zealand formed an alliance (Five Eyes) based on a series of bilateral agreements on surveillance and intelligence-sharing. This series of agreements enabled States to share intelligence gathered and decrypted by each of their intelligence agencies by default. While the agreements underlying Five Eyes are not in the public domain, the concern among critics is that the involvement of foreign intelligence agencies in intelligence sharing allows domestic agencies to gain information they could not access themselves without violating domestic legal restrictions on state surveillance.[1]

As technological developments picked up pace, the so-called *crypto-wars* began in the 1970s when the US government attempted to classify encryption as munitions - as a technology recognised and regulated as a weapon of war. The origins of the securitisation and desire to control online space by states have been there from the beginning, and are an important part of understanding why there is widespread criticism of any proposals that undermine or seek to ban the use of encryption today.

In the early days of the expanding commercial Internet, encryption was a technology that companies in the US could choose to use in products they built and exported. But the US government passed legislation to limit the use of cryptography both in terms of export controls, preventing the export of physical products and software to markets outside of the US that used a strong level of encryption in security-by-design, and also by creating domestic requirements to enable state access to digital content of communications.

1 See: https://privacyinternational.org/learn/five-eyes

As the US debate grew on how to charge for telephony[2] in the earlier days of the Internet, a wider range of politicians and governments became involved due to the economic implications and concerns about domestic sovereignty.

Author Wendy Grossman foresaw, writing in 1997, that the technological "Silicon Valley" hype driving the claim that the new medium of communication was going to "remake the world, undermine the status quo and kill off national governments and multinational corporations" would inevitably lead to the imposition of State governance and controls. Even then, nearly thirty years ago, when the majority of people were not yet online, those controls were being talked about as governance that would shape the Internet to fit politicians' idea of "something that's safe."[3]

This definition of "safety" online was contentious even then. Safe for whom and from what?

In the 1980s, as the Crypto Museum website explains,[4] when computers were beginning to emerge in commercial companies after being previously exclusive to military environments, it became increasingly necessary for wireless and wired links to carry not only the data of a single computer, but complete *data bundles*, from multiple devices simultaneously, often including speech and facsimile (fax) data. Such devices are commonly known as bulk encryptors. The required equipment was bulky and needed manual actions like turning encryption on and off, or using an electronic device for the distribution of cryptographic variables, such as crypto keys.

During the 1990s, the World Wide Web led to a huge increase in the amount of information available to "non-technical" people via the Internet. This decade also saw the rise of e-commerce and the advent of "easy" encryption at scale by the technically minded masses, through pretty good privacy (or PGP as it's known). This is a tool that enables users to communicate securely by decrypting and encrypting messages, authenticating messages through digital signatures, and encrypting files.

With the growing use of the personal computer, the US government then tried to create a physical route to enable the government to always have access to a key to encrypted communications, using the so-called Clipper Chip, that allowed "back door" access into transmissions from any device built using the chip. There was a process by which government agencies could establish their authority to intercept a particular communication, and then the key held in escrow by a third-party would be given to that agency, so that all data transmitted could be decrypted. Law enforcement and agencies desiring access to the contents of the message could then approach the third-party without notifying the key's owner.

2 Telephony is technology associated with interactive communication between two or more physically distant parties via the electronic transmission of speech or other data: https://www.techtarget.com/searchunifiedcommunications/definition/Telephony

3 Grossman, W., *net.wars*, 1997, New York University Press, p. 196, https://nyupress.org/9780814731031/net-wars

4 See: https://www.cryptomuseum.com/crypto/index.htm

But in response to the threat of the US Government passing legislation to ban encryption, a number of very strong *public* encryption packages were released, including Nautilus, PGP and PGPfone. It was thought that, if strong cryptography was widely available to the public, the government would be unable to stop its use. This approach appeared to be effective, and notwithstanding that a flaw meant it was compromised, the life of the Clipper Chip was limited, broken in 1994.

These government policy proposals created repeated contention. Wendy Grossman said in an interview for this report, "Is it any wonder that the Net feels under siege? Is it surprising that feeling threatened further bonds the community together, and that some elements unite in a determination to see that attempts at regulation fail? Regulating cyberspace is a lot like shooting the messenger."[5]

By 1999 there was consensus among technologists, as well as politicians who championed free market libertarian principles, that the imposition of export controls meant the US had exported devices that were not as secure as they should have been. Matt Blaze, who exposed the failings of the Clipper Chip[6] among his extensive work in cryptography, describes this period as one in which "'crypto' [was] misguidedly derided as some kind of criminal tool during the very time when we needed to be integrating strong security into the Internet's infrastructure," and that it set back Internet security "by at least a decade, and we're still paying the price in the form of regular data breaches, many of which could have been prevented had better security been built in across the stack in the first place."[7]

After the attempt to create these keys giving "back door" access into exported technology had failed, the security services tried another method: getting into commercial companies that created secure SIM cards for mobile devices. Whistle-blower Edward Snowden, working for the US National Security Agency (NSA), revealed documents in 2015 that allegedly show that the NSA and their British counterpart GCHQ hacked the French-Dutch smart-card company called Gemalto to acquire the cryptographic keys of millions of mobile phone SIM cards.[8] It is unknown how many keys were stolen or how efficient the application of such keys would be but it was claimed that it allowed access to those SIM card users in predominantly 2G environments like Pakistan.

However encryption experts, digital rights advocates, and tech companies all agree that there is no safe backdoor to encryption.

5 CRIN and ddm interview with Wendy M. Grossman, 28 September 2022.

6 Callas, J., *The Recent Ploy to Break Encryption Is An Old Idea Proven Wrong*, 23 July 2019, https://www.aclu.org/news/privacy-technology/recent-ploy-break-encryption-old-idea-proven-wrong

7 Blaze, M., *Exhaustive Search has Moved*, 7 July 2018, https://www.mattblaze.org/blog/newaddress/

8 See the Crypto Museum website on Gemalto: https://www.cryptomuseum.com/manuf/gemalto/index.htm

> *"Any backdoor would create more security risks, including for individual users, than it would solve. Any friction in the message transmission chain, or security vulnerabilities in the encryption protocol, risks being exploited by adversarial (state and non-state) actors."*[9]

If a back door is created to give "exceptional access" for law enforcement, it is a backdoor for any third party to access the contents of communications. This might sound harmless, but the results can be disastrous, according to the Internet Society.[10]

The Electronic Frontier Foundation has pointed out that the US government has not been shy about seeking access to encrypted communications, pressuring the companies to make it easier to obtain data with warrants and to voluntarily turn over data. However, the US would face serious constitutional issues if it wanted to pass a law that required warrantless screening and reporting of content.[11]

Only a decade ago, Lavabit, an open-source encrypted webmail service founded in 2004, suspended its operations on 8 August 2013 after the US Federal Government ordered it to turn over its Secure Sockets Layer private keys, in order to allow the government to spy on Edward Snowden's email.

Newer proposals from agencies have included rather more transparent discussions. The most recent proposals have moved to new points in the process to eavesdrop or report recognised content. But the principle remains the same, that they enable eavesdropping or report the user to a third-party.

The proposal that followed in 2019 from GCHQ, was to permit law enforcement and intelligence agencies access to private messaging systems by adding a silent participant––"ghost" users from law enforcement or the security services–– to online chats and calls, including those conducted via encrypted messaging tools like WhatApp, iMessage, or Signal. The "ghost proposal"[12] was widely condemned in 2019, including by the Internet Society,[13] as the latest attempt by a government to circumvent and/or "backdoor" encrypted communications and was reminiscent of the aims of the Clipper Chip. A coalition of more than fifty civil society organisations, technology companies and cybersecurity experts including Apple, Microsoft, Human Rights Watch and Privacy International wrote in objection to the proposals that this would "open the door to surveillance abuses that are not possible today."[14] Not only did it create current risk, it would require companies to keep that risk open, and not "patch" the weakness, which others could also exploit.[15] By inserting tools for surveillance into products, states would effectively limit security innovation, just as was seen as a result of the US government export controls of the 1990s.

Where that leaves us today

Understanding the origins of the "cyber wars" and long-running debates on state surveillance, with the associated outcomes for individuals and at scale, may go some way to understanding today's tensions showing why the technology solutions used and proposed policy approaches have reached somewhat of a stalemate.

A key faultline between those who argue that communications should be encrypted to protect content from prying, and those who argue it should not be encrypted so that state agencies can access the content of any exchange of information rests on one key issue: the harm that governments and their state bodies perpetuate to populations at scale, and the resulting lack of trust in government agencies and law enforcement that have developed over time.

It is also important to recognise that the push by States to restrict encryption have been, and continue to be, pursued for a number of different purposes globally and have changed over time. The current focus of emerging EU regulation is on child sexual abuse material, in the US counter-terrorism was a driving force for reform since 9/11. In Brazil the government has claimed[16] it is essential to fight crime, bribery and corruption,[17] while in India, mob violence and the connections with misinformation are the current policy drivers.

Privacy in the digital environment is no doubt one of the most important factors in how we enable and control individuals and societies. Today's children may be the first generation in which the perfect storm of ubiquitous digital information and ubiquitous state and commercial surveillance combine. This is the context in which the debate about regulation of encryption takes place as well as the analysis of how to do so in a way that respects children's rights.

9 Tech Against Terrorism, *Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies*, 2021, https://www.techagainstterrorism.org/wp-content/uploads/2021/09/TAT-Terrorist-use-of-E2EE-and-mitigation-strategies-report-.pdf

10 ISOC, *Breaking Encryption Myths: What the European Commission's leaked report got wrong about online security*, 2020, https://www.internetsociety.org/resources/doc/2020/breaking-the-myths-on-encryption/

11 EFF, *If You Build It, They Will Come: Apple Has Opened the Backdoor to Increased Surveillance and Censorship Around the World*, 2021, https://www.eff.org/deeplinks/2021/08/if-you-build-it-they-will-come-apple-has-opened-backdoor-increased-surveillance

12 Levy, I. and Robinson, C., *Principles for a More Informed Exceptional Access Debate*, 2018, https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

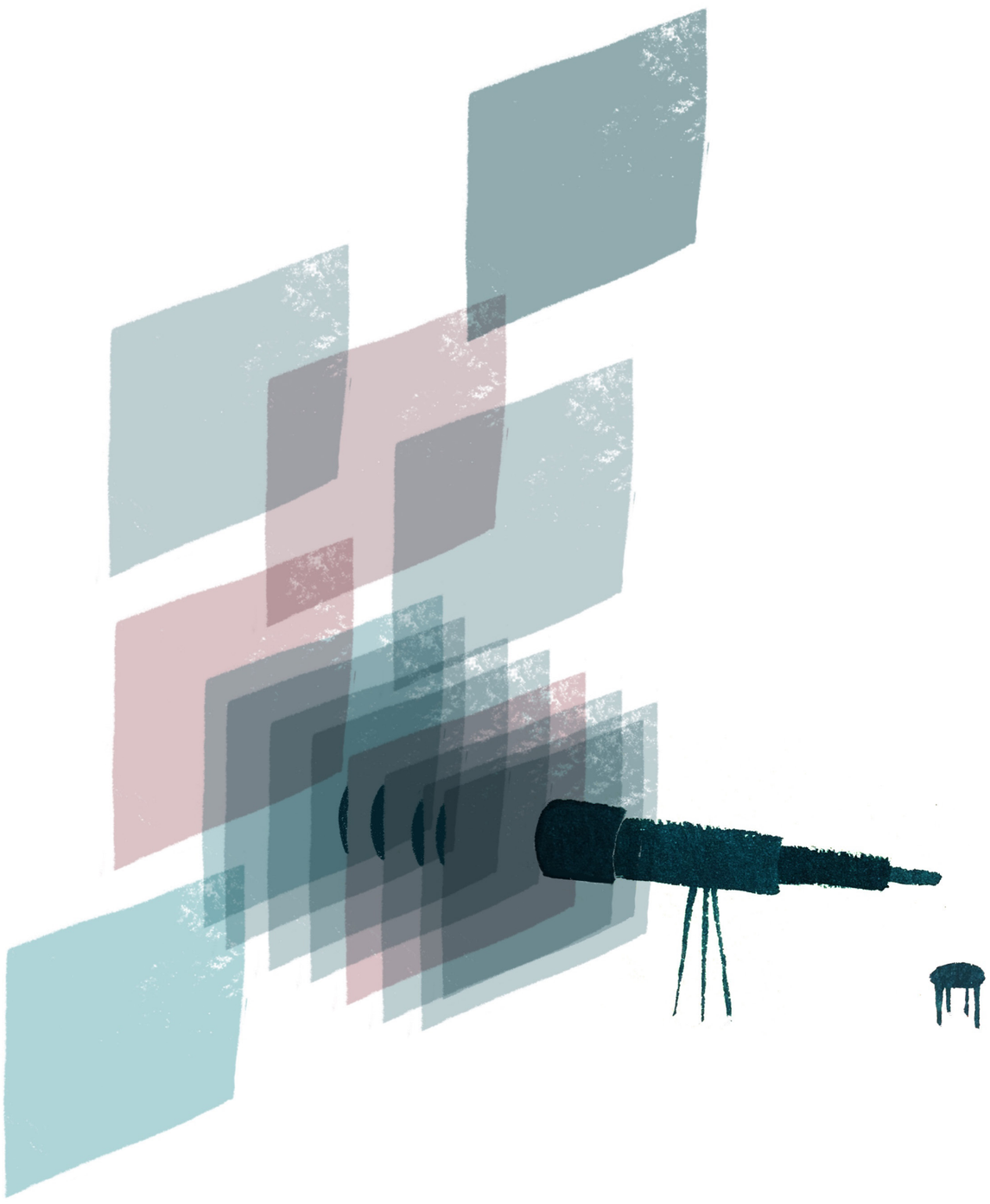
13 ISOC, *Ghost Protocol Fact Sheet*, 2020, https://www.internetsociety.org/wp-content/uploads/2020/03/Ghost-Protocol-Fact-Sheet.pdf

14 Clayton Rice, K.C., *The Ghost Key Proposal*, https://www.claytonrice.com/the-ghost-protocol/

15 Green, M., *On Ghost Users and Messaging Backdoors*, 2018, https://blog.cryptographyengineering.com/2018/12/17/on-ghost-users-and-messaging-backdoors/

16 See Riana Pfefferkorn regarding Operation Car Wash in this event organised by the Stanford Cyber Policy Center: https://www.youtube.com/watch?v=K0myjgC3Aho&ab_channel=FSIStanford

17 Fishman, A. et al., *The Secret History of US Involvement in Brazil's Scandal-Wracked Operation Car Wash*, 12 March 2020, https://theintercept.com/2020/03/12/united-states-justice-department-brazil-car-wash-lava-jato-international-treaty/



Understanding encryption and its place in the digital environment

Developing a children's rights approach to encryption requires a thorough understanding of the technology: how it works, how it is used and how it is integrated into the digital environment. When it comes to decisions of if and how to apply encryption, there are consequences at the individual, community, institutional, State and international levels.

Some regulators have recognised that each provider is different, with different architectures, business models and user bases. This means that an intervention, or use of specific tools on one platform, may not be proportionate on another.[18] This is why it is important to set out the technology and explore the differences and nuances in technical discussions.

There has often been talk of "strong encryption" or "breaking encryption" or "workarounds" of encryption in recent debate. What do these really mean in everyday language? Why does it matter in the current debate around children in the digital environment?

Encryption and the Internet

To understand what encryption is and why it matters one should first understand some basic workings of the Internet and the World Wide Web.

Becky Hogge's guide, *Internet Policy and Governance for Human Rights Defenders*,[19] offers a useful explainer of the construction of the Internet and how the World Wide Web runs on it, described in seven separate layers, each one "stacked" upon the last.[20] The model helps to give a sense of place to everyday users, the actors and stakeholders involved in each part of its design, development, maintenance and existing governance models.

Almost all of the recent debate in the Anglo- and Euro-centric spaces on "encryption", "platforms" and children only considers the content, users, and their

18 Australian eSafety Commissioner, *Basic Online Safety Expectations. Responses to transparency notices*, 2022, https://www.esafety.gov.au/industry/basic-online-safety-expectations/responses-to-transparency-notices

19 Hogge, B., *Travel Guide to the Digital World: Internet Policy and Governance for Human Rights Defenders*, 2014, https://www.gp-digital.org/wp-content/uploads/2014/06/Travel-Guide-to-the-Digital-Worlds-1.pdf

20 See: https://computersciencewiki.org/index.php/OSI_model

interactions in the one superficial layer where content can be viewed. But secure methods of managing different parts of the Internet rely on encryption throughout the full set of layers, or the "stack" of its construction. This is why some people say, for example, that if you ban encryption online you prevent secure banking or commerce.

As Hogge described in her guide,[21]

> *"Network operators can censor and monitor content at the physical layer. At the code layer, the IETF and ICANN set standards and maintain the key functions of the internet. The application layer is host to huge technology companies such as Google and Facebook, whose market dominance has conspired to make their services the "town squares" of the digital age."*
>
> Becky Hogge, *Internet Policy and Governance for Human Rights Defenders*

How does communicating on the World Wide Web work?

Simplistically speaking, data is sent across the Internet in "packets" from one digital device to another, broken up into manageable parcels that flow in a stream of traffic of electronic data. But just like anything that is sent into the postal service, the sender cannot control what happens to the parcel once it is sent. There are therefore switches and agreements that are used to instruct each part of the system how to handle and distribute the packets. Those instructions need to be readable and understood across the whole World Wide Web, so the administrative functions and tasks are coded in broadly accessible instructions across the Internet. These standards are being constantly refined, improved and new standards designed where needed.

Each packet of information can be sent in a variety of ways, and can be sent "in the clear" so that anyone with access to the packet at any point in its journey can also see into its contents, in effect distributing an open letter without an envelope.

Alternatively, the sender and recipient may encode the data through encryption, which is commonly thought of as a method used to preserve confidentiality between parties who want to send, share or store information without it all being visible from the outside. In this sense, encryption is used to protect the contents of the transmitted data, but it is also possible to protect the transport tool, not only what is inside it.

This is where the term "metadata" matters, which is in effect the labelling and descriptive information added to the outside of the packets, including the addresses of the sender and recipient, that enable the packets to all arrive in the same place and be put back together in the correct order for the recipient to receive and read as the sender intended.

> When encryption is used "in transit" with the intention to prevent third parties who might intercept the content of the data packets from being able to read it while it is moved from one place to another and it can only be read by the sender before it is sent or after it is received by the recipient, it may be called "end-to-end" encryption.

> *"The internet has been called a "world of ends" and an "end-to-end network", because on the internet the stuff that matters, the smart stuff, happens at the end points, at the computers that connect to it. The computers that connect to the internet are constantly generating, storing and sharing information."*
>
> Becky Hogge, *Internet Policy and Governance for Human Rights Defenders*

An important caveat should be remembered when defining what end-to-end encryption means in practice. If the servers, sending, storing and receiving data, control the encryption keys - the keys used to decode the data - that are used on the servers and not the end users themselves, the server operator will have access to data. The environment is therefore not controlled by the users' choices about encryption and the server controller will be able to access its content and provide it to law enforcement upon request.

What does encryption do for me in the World Wide Web?

Encryption is a fundamental part of creating secure websites. However, recent advances in webpage security have led some to argue end-to-end encryption is detrimental to protecting children online.

When users visit a web page, they see data that is hosted on that website because electronic information is transferred between where it is stored to the user's "browser" (e.g. Google Chrome, Microsoft EDGE, Mozilla Firefox). But how does a computer find which site is the one that you want among the billions of webpages in the world?

The Domain Name System ("DNS") is a system for naming and identifying computers reachable through the Internet or other Internet Protocol networks. It is the system that enables humans to look up a web address and get what we know as domain names (e.g. https://home.crin.org/) "resolved" into numerical IP addresses that the computer can find (i.e. 198.185.159.144) and back again.

21 Hogge, B., *Travel Guide to the Digital World: Internet Policy and Governance for Human Rights Defenders*, 2014, p. 46.

This naming system exists to make finding websites easier for people, who generally find it difficult to remember long strings of numbers. DNS acts as an address book that humans and computers can both understand.

Various browser companies have upgraded user security in recent years to ensure that they use DNS over https (DoH). This means that data is encrypted when it is transferred from the computer where it is stored to the browser of the person viewing the website. Websites that use this kind of protection (called SSL/TLS) start with "https" rather than "http". This development is intended to make accessing websites more secure, by preventing false authentication by "man-in-the-middle attacks".

Man-in-the-middle attacks refer to situations where a stranger interferes with data that is being transferred, for example by pretending to show users the website they are trying to visit, but changes important details. The attacker could point the data entry of credit card details of the user to a different end point as a way of stealing (or "phishing") personal and financial information.

Cloudflare, a global cloud services provider, explains it like this:[22]

> *"SSL ensures that anyone who intercepts the data can only see a scrambled mess of characters. The consumer's credit card number is now safe, only visible to the shopping website where they entered it."*
>
> *"SSL also stops certain kinds of cyber attacks: It authenticates web servers, which is important because attackers will often try to set up fake websites to trick users and steal data. It also prevents attackers from tampering with data in transit, like a tamper-proof seal on a medicine container."*

Website encryption and the challenges of identifying illegal and harmful content

The shift to greater security of websites through "https over DNS" or "DoH" has created challenges for some organisations responsible for creating lists of websites to be blocked or monitored. For example, the UK's Internet Watch Foundation (IWF) scans webpages to create lists of websites containing illegal or harmful content for children, including related to terrorism or pornography. This makes it possible to block sites containing this content and the creation of watchlists so that others can monitor when their users are accessing this kind of material.

In February 2020, Firefox switched to DNS over https by default for users in the US making their default browsing experience more secure. According to John Dunn writing for Sophos,[23]

> *"[T]o privacy enthusiasts, this change was good because neither [Internet Service Providers] nor governments have any business knowing which domains users visit. For ISPs, by contrast, DoH hands them several headaches, including how to fulfil their legal obligation in the UK to store a year's worth of each subscriber's internet visits in case the government wants to study them later for evidence of criminal activity."*

The UK is already recognised as having one of the more intrusive approaches to state demands made of Internet Service Providers. Companies that want to promote the more secure web architecture, "https over DNS", include DNS providers that offer filtering and parental controls. However, the Internet Service Providers Association (ISPA)[24]—a trade association representing British ISPs— and the British Internet Watch Foundation have both criticised Mozilla, the not-for-profit organisation behind the Firefox browser, for supporting DoH, saying that it will undermine web blocking programs including ISP default filtering of adult content, and mandatory court-ordered filtering of copyright violations which rely on less secure architectures to be effective.[25] Mozilla subsequently said that DoH will not be used by default in the British market until further discussion with relevant stakeholders, but stated that were it implemented, it "would offer real security benefits to UK citizens".[26]

In fact, this workaround is exploited by some companies, for example those that sell web filtering (and user monitoring) systems and services to educational settings. They in effect pose as the real website, but impersonate it.

To filter out content, means first having access to it. Filters essentially come in one of three types, according to Professor Ross Anderson,[27] depending on which level they operate at. Packet filtering, circuit gateways (where DNS filtering happens), and application proxies (mail filters that try to weed out spam). Since the adoption of more secure transport routes via https, the tools that perform such jobs have been pushed to the endpoints of systems and networks.

Encryption alone does not protect confidentiality or commercial practice or the contents of communications. It only protects against unwanted third-party observers. It does not guarantee what the individuals or institutions—the "endpoints"—then do afterwards, with the (now decrypted) data.

This is especially important to remember when considering whether one method of encryption is more "privacy-preserving" than another, or in evaluating whether a particular technological intervention at one point in the process does or does not

22 See: https://www.cloudflare.com/en-gb/learning/ssl/what-is-ssl/

23 Dunn, J., *ISPs call Mozilla 'Internet Villain' for promoting DNS privacy*, 2019, https://nakedsecurity.sophos.com/2019/07/08/isps-call-mozilla-internet-villain-for-promoting-dns-privacy/

24 ISPA, *ISPA withdraws Mozilla Internet Villain Nomination*, 2019, https://www.ispa.org.uk/ispa-withdraws-mozilla-internet-villain-nomination-and-category/

25 See: https://en.wikipedia.org/wiki/DNS_over_HTTPS

26 The Guardian, *Firefox: 'no UK plans' to make encrypted browser tool its default, 2019*, https://www.theguardian.com/technology/2019/sep/24/firefox-no-uk-plans-to-make-encrypted-browser-tool-its-default

27 Anderson R., *Security Engineering—A Guide to Building Dependable Distributed Systems*, 2020, Chapter 21, https://www.cl.cam.ac.uk/~rja14/book.html

"interfere" with privacy. Encryption is not a single tool at a single point of a physical process, but multiple types may be involved in any one online communication. The principle and practice at stake are whether there is any interference by any third party at all.

Why does understanding this matter? Because encryption is necessary for keeping users safe online and discussions that paint 'encryption' only as a threat make finding workable solutions to address the real problems more difficult. As described by Dr. Ian Levy and Crispin Robinson of GCHQ in 2018 in an article on Lawfare[28]:

> *"Collectively, we've defined the various different service and device problems as a single entity called 'encryption.' That's unhelpful as the details of each device and each service will constrain and drive particular solutions."*

Encryption and metadata

Metadata is information about other data. In the conversation about digital communications, metadata can include information about where data came from, its structure, storage and how it is shared. For example, if data originated from a mobile phone, the metadata might include the name, model, firmware, type of device, configuration and capacity of that phone.

Metadata usually includes information useful to the providers of services used in the communications process, such as how well it is performing, how fast information is being written or read and how quickly systems are responding. For example, if the information that is transmitted includes audio or video, it is important for service providers to optimise the speed and order in how packets of data are sent, arrive and are reconstructed to improve the experience of users. Metadata will also include information about the servers, computers and other devices where data came from, has gone to and is stored.

Encryption that protects the contents of communication does not protect the metadata which the sender and recipient did not create but without which the packet cannot pass through different parts of the system because the routing information needs to be readable for the message to get to the right destination.

On WhatsApp, content and metadata[29] are both encrypted, which means artificial intelligence systems cannot scan all chats, images and videos automatically as they do on Facebook and Instagram. However, the metadata is still visible to the parent company Meta so that it can direct the messages to the right user. It can also access content information if users back up their WhatsApp messages and interact with a business account on the platform.[30] Content moderation reviewers can gain access to communications when users engage the "report" button on the app, and claim a message is violating the platform's terms of service, including sextortion, since 2020.[31]

Metadata is intended for reading by machines, but because metadata is very detailed it can also be used to tell people a lot about the relationship and behaviours of the parties involved in any digital activity or communications, even without seeing what is contained in the content.

When digital publishing companies add metadata onto academic papers or educational materials to catalogue the attributes of contents of libraries, it is used by automated search engines to identify, profile and find materials that match search criteria in all of the content of billions of Internet page searches for example. In similar ways, metadata about communications may be used to identify, profile and find individual people talking to each other among the billions of people online in the world.

David Cole, the National Legal Director of the ACLU and the Honorable George J. Mitchell Professor in Law and Public Policy at the Georgetown University Law Center memorably quoted the NSA General Counsel Stewart Baker in a debate in 2014, saying, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content", to explain how metadata alone can provide an extremely detailed picture of a person's most intimate associations and interests. It is much easier as a technological task alone to search huge amounts of metadata than to listen to millions of phone calls. His co-panellist in the debate General Michael Hayden, former director of the NSA and the CIA, called Baker's comment "absolutely correct" and added, "We kill people based on metadata."[32]

The UN High Commissioner for Human Rights described in 2018, why the question of confidentiality applies to both the contents of communications and the metadata, "The protection of the right to privacy is broad, extending not

28 Levy, I. and Robinson, C., *Principles for a More Informed Exceptional Access Debate*, 2018.

29 WhatsApp Encryption Overview Version 6 Updated November 15, 2021. Communication between WhatsApp clients and WhatsApp chat servers is layered within a separate encrypted channel using Noise Pipes with Curve25519, AES-GCM, and SHA256 from the Noise Protocol Framework. https://web.archive.org/web/20221130062942/https://scontent-lcy1-1.xx.fbcdn.net/v/t39.8562-6/309473131_1302549333851760_6207638168445881915_n.pdf?_nc_cat=107&ccb=1-7&_nc_sid=ad8a9d&_nc_ohc=kqXq2gkRQegAX_fbxBa&_nc_ht=scontent-lcy1-1.xx&oh=00_AfDWug1Zxaocf-mudtpA4Y7fhIifJV3WcpTK4H8C6Tl4kA&oe=638BB35D; See Mooney, N., *An Introduction to the Noise Protocol Framework*, 2020, https://duo.com/labs/tech-notes/noise-protocol-framework-intro

30 Cloud API, operated by Meta, acts as the intermediary between WhatsApp and the Cloud API businesses. In other words, those businesses have given Cloud API the power to operate on their behalf. Because of this, WhatsApp forwards all message traffic destined for those businesses to Cloud API. WhatsApp also expects to receive from Cloud API all message traffic from those businesses: https://developers.facebook.com/docs/whatsapp/cloud-api/overview/data-privacy-and-security

31 ProPublica, *How Facebook Undermines Privacy Protections for Its 2 Billion WhatsApp Users*, 2021, https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users

32 Cole, D., '*We Kill People Based on Metadata*', 2014, https://www.nybooks.com/online/2014/05/10/we-kill-people-based-metadata/. The full comments can be heard in the context of the debate at: https://www.youtube.com/watch?v=kV2HDM86XgI.

only to the substantive information contained in communications but equally to metadata as, when analysed and aggregated, such data 'may give an insight into an individual's behaviour, social relationship, private preference and identity that go beyond even that conveyed by accessing the content of a communication'". [33]

Using metadata to identify online child sexual exploitation and abuse

The potency of metadata is one reason that technologists argue that it is not necessary or proportionate to access the content of everybody's communications through mass surveillance, because metadata can indicate patterns of contact of behaviour that gives away a great deal of information about illegal activities. Some argue that metadata should be used to identify and justify where targeted interventions can be made to access content, based on suspicion, rather than mass surveillance or interception, subject to judicial oversight.

This process can also work in reverse. According to Dr. Ian Levy and Crispin Robinson of GCHQ, in all cases, once an image is determined to be child sexual abuse imagery, the service provider knows from the service *metadata* the identities of those accounts that shared the content, those that received it and those that re-shared it. This knowledge means that educational messages could be targeted at the relevant users and, if necessary, search warrants taken against users who offend in this way.[34] The power of potential uses of metadata have led some actors engaged in online regulatory reform to suggest a higher level principle around using reasonable efforts to identify child sexual abuse material:

> *"Every platform comprises various different kinds of metadata, collects it, assesses it in particular ways. Metadata can only ever suggest that something is illegal or harmful, it cannot tell you with any certainty. [...] All it can do is say that there are factors which indicate that there might be something illegal or harmful, and then you have to do a human review. And those factors and the weighting they have vary massively from platform to platform. So it is a very difficult thing to regulate on an industry-wide level, and I'm not sure regulation needs to be so specific around the use of metadata. [...] [But it could] require platforms to use reasonable efforts to identify [child sexual abuse material] and then a regulator can make an assessment as to whether a company is doing that, whether it's using the metadata that it does collect in the most effective way, and require the company to take further steps if it's not doing so."*[35]

> *"It's a very powerful tool, looking at metadata, it's potentially very intrusive. We definitely are strongly against the bulk collection or scanning of metadata. Metadata would need to be used in a very targeted fashion, which means that other techniques would first need to be used to identify the suspects. This is, I think, not the way that a lot of people see metadata as solving this problem, because they want to use it in bulk and do big analyses and pattern matching to try to find potentially suspicious individuals."*[36]

> *"Lots of metadata is generated [...] I think it's one of a number of approaches that companies should be working on improving [...] Even if it still leaves significant gaps, I think it's important to have a process with governments to think about how companies might make more effective use of it without compromising people's rights."*[37]

Uses of encryption beyond confidentiality

Encryption has value and uses that go beyond protecting confidential information. The importance of understanding how the applications of encryption go beyond keeping things confidential is vital in the analysis of risks and benefits, according to UK-based technology lawyer, Neil Brown:

> *"[I]f you are solely focussed on providing a 'good enough' solution to confidentiality, and you ignore the other facets of encryption, your solution is likely to be inadequate."*[38]

He identifies twelve areas where encryption plays a role, in addition to confidentiality, including:

- **Anonymity**: keeping the identity of a party unknown to the other party or parties, or to one or more service providers;
- **Asynchronicity**: the ability for someone to send a message, even though their intended recipient is offline, or for someone to receive a message, even though the sender of that message is offline; and
- **Authentication**: checking that the encrypted information was encrypted correctly, using the chosen encryption algorithm.

33 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29, 3 August 2018, para. 6, https://www.ohchr.org/en/documents/reports/ahrc3929-right-privacy-digital-age-report-united-nations-high-commissioner-human

34 Levy, I. and Robinson, C., *Thoughts on child safety on commodity platforms*, 2022, p. 64, https://arxiv.org/pdf/2207.09506.pdf

35 CRIN and ddm interview with Richard Wingfield, 6 September 2022.

36 CRIN and ddm interview with Privacy International, 26 September 2022.

37 CRIN and ddm interview with Ian Brown, 6 October 2022.

38 Brown, N., *The end to end encryption debate: 1: the (very) basics of "encryption"*, 2022, https://neilzone.co.uk/2022/01/the-end-to-end-encryption-debate-1-the-very-basics-of-encryption

Most importantly, "encryption" is not a single technology or even collection of different tools. Brown describes "encryption" as a concept, or set of processes within a system. In practice, the process of encryption is carried out through algorithms, and not all algorithms are the same, or attempt to do the same things. Some algorithms have different capabilities and are better suited to one task above another. Some algorithms demand more from the users than others e.g. more computational resources, or more technical skill to apply.[39]

Encryption in children's everyday lives

Children benefit from the use of encryption as applied in their everyday life in cyber security and privacy, as adults do. A common thread across the domains of child safety and privacy might be considered a question of interference. Who may interfere with a child and their full and free development, their everyday activities and communications, how, with what effect, and for what purposes?

The domains in which security may protect children and keep them safe, where they are active online include not only communications and social media, but access to finance, health, education, politics, participation in culture, community, and play. Across these environments, insecure technology has had a significant impact on children.

In 2011, 77 million Sony PlayStation user details were reported stolen. The "illegal and unauthorised person" obtained people's names, addresses, email addresses, birth dates, usernames, passwords, logins, security questions and more, Sony reported, and children with accounts established by their parents also might have had their data exposed.[40]

In 2015, children's technology and toy firm Vtech suspended trading on the Hong Kong stock exchange after admitting a hack that allegedly saw 5 million customer details stolen, including sensitive information and unencrypted chat logs between children and their parents.[41]

39 For more information on the breadth of technical and policy concepts regarding encryption, see: UK Information Commissioner's Office, *What is Encryption?*, 2022, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/what-is-encryption/

40 Reuters, *Sony PlayStation suffers massive data breach*, 27 April 2011, https://www.reuters.com/article/us-sony-stoldendata-idUSTRE73P6WB20110427

41 VICE, *One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids*, 27 November 2015, https://www.vice.com/en/article/yp3z5v/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids. The breach of the popular kids' gadgets company VTech also exposed children's pictures and recordings, and chats with their parents: VICE, *Hacker Obtained Children's Headshots and Chatlogs From Toymaker VTech*, 30 November 2015, https://www.vice.com/en/article/yp3zev/hacker-obtained-childrens-headshots-and-chatlogs-from-toymaker-vtech

In 2016 the Norwegian Consumer Council (NCC) identified problems in Internet connected toys that are emblematic of the increased spread of connected devices. The NCC said that in a growing market, it is essential that consumers, and especially children, are not being used as subjects for products that have not been sufficiently tested.[42]

In 2017 together with the security firm Mnemonic, the NCC also tested several smartwatches for children. The researchers discovered significant security flaws, unreliable safety features and a lack of consumer protection. Finn Myrstad, the Director of Digital Policy at the Norwegian Consumer Council, said at the time that,

> *"It's very serious when products that claim to make children safer instead put them at risk because of poor security and features that do not work properly."*[43]

In the educational environment, the US Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) acknowledged in 2022 that educational settings are high risk for ransomware attacks, where limited cybersecurity capabilities and constrained resources increase settings vulnerability and "K-12 institutions may be seen as particularly lucrative targets due to the amount of sensitive student data accessible through school systems or their managed service providers."[44]

In the family environment a child may experience a conflict between their own agency and the rights and responsibilities of the parent, particularly in culturally conservative households. These considerations are most relevant when considering parental monitoring or control services on children's phones and other devices. In order to offer parents surveillance or monitoring services over their children's mobile devices, parental control apps require privileged access to system resources and access to sensitive data.

According to Feal, "this may significantly reduce the dangers associated with kids' online activities, but it raises important privacy concerns. These concerns have so far been overlooked by organizations providing recommendations regarding the use of parental control applications to the public."[45]

42 See: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

43 See: https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/

44 US Cybersecurity and Infrastructure Security Agency, *Alert (AA22-249A) #StopRansomware: Vice Society*, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-249a.

45 Feal, Á. et al., *Angel or Devil? A Privacy Study of Mobile Parental Control Apps*, 2020, Proceedings on Privacy Enhancing Technologies 2020 (2): 314 - 335, https://petsymposium.org/popets/2020/popets-2020-0029.php

In a review of 3,264 parental control apps conducted in 2021, researchers Wang et al. found that they were being increasingly adopted by parents as a means of safeguarding their children's online safety.[46] However, it was not clear whether these apps are always beneficial or effective in what they aim to do; for instance, the overuse of restriction and surveillance has been found to undermine the parent-child relationship and children's sense of autonomy. Ghosh et al. had found in 2018 that overall, increased parental control was associated with more (not fewer) online risks.[47]

Dr Ian Levy and Crispin Robinson also point out in their most recently published paper:

> *"[T]his kind of mechanism may place some children at additional risk from abusive or manipulative parents, even when the parents themselves don't have access to content, and whilst the technique would be technically relatively straightforward to scale, research would be necessary to determine how well it would be likely to cover the users most at-risk and how at-risk children could be effectively protected."*

Security is a process, not a product. Encryption may turn trust into machine-readable code so that machines can verify and trust each other, but human trust still relies on one another. Using tools to replace that has consequences.

Scanning unencrypted content to match known images

Technological developments have enabled new routes to access and abuse children at scale both in real-time and through repeated distribution of content and so, in turn, new technology is being developed and applied to respond to these challenges.

When it comes to detection and content moderation, to identify and remove images of child sexual abuse, the best known technology is PhotoDNA, created by Professor Hany Farid and owned by Microsoft.

PhotoDNA[48] works by creating a unique digital signature (known as a "hash") of an image which is then compared against hashes of other photos to find matching copies of the same image. This is deployed in an *unencrypted* environment. Facebook adopted the use of PhotoDNA in 2010 across its entire network, Twitter in 2011 and Google in 2016.[49] The software operates in unencrypted environments, such as in the open web without https, non-end-to-end encrypted channels or at points where content is stored in unencrypted form (i.e. at the level of Internet Service Providers).

In 2018, when deploying PhotoDNA, and to avoid the complexity of classifying content whose legality might be disputed, Facebook policy was to "only add content to the database that contains images of children *under the age of 12* involved in an explicit sexual act".[50] In 2019, Facebook moved to a different hashing algorithm, PDQ, which they developed themselves and a version of which will also hash video.[51]

The most common criticism of PhotoDNA, is that it only knows what it knows. PhotoDNA will not detect previously unreported or new images. Despite this, former President and CEO of the National Center for Missing and Exploited Children Ernie Allen says it is an important tool in content removal to reduce victimisation, and can identify photos that have been in circulation for many years, or that are new but have been identified and turned into a hash only recently. "Using PhotoDNA, we will be able to match those images, working with online service providers around the country, so we can stop the redistribution of the photos."[52]

Professor Farid has also built a modified version of photoDNA, called eGlyph, for the identification of material for counter-terrorism purposes. It is worth drawing attention to his own comments made in his 2018 paper, that the application to target any particular kind of image, or person, is not limited by safeguards built into the technology, but by policy:

> *"[A]ny technology such as that which we have developed and deployed can be misused. The underlying technology is agnostic as to what it searches for and removes. When deploying photoDNA and eGlyph, we have been exceedingly cautious to control its distribution through strict licensing arrangements. It is my hope and expectation that this technology will not be used to impinge on an open and free internet but to eliminate some of the worst and most heinous content online."*

The concern is widespread among privacy experts that policy safeguards provide insufficient protection against the increased scope for usage of the technology beyond the identification of child sexual abuse images.

46 Wang, G. et al., *Protection or punishment? Relating the design space of parental control apps and perceptions about them to support parenting for online safety*, 2021, Proceedings of the Conference on Computer Supported Cooperative Work Conference, 5(CSCW2), https://ora.ox.ac.uk/objects/uuid:da71019d-157c-47de-a310-7e0340599e22

47 Ghosh, A. et al., *A Matter of Control or Safety?: Examining Parental Use of Technical Monitoring Apps on Teens' Mobile Devices*, 2018, Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, https://www.semanticscholar.org/paper/A-Matter-of-Control-or-Safety%3A-Examining-Parental-Ghosh-Badillo-Urquiola/67ed9c02529ecfba7fe35cf8ec1bfdc42dbc73c8

48 See Microsoft on PhotoDNA: https://www.microsoft.com/en-us/photodna

49 Farid, H., *Reining in Online Abuses*, 2018, Technology & Innovation, 19(3) 593–599.

50 Ibid.

51 Meta, *Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer*, 1 August 2019, https://about.fb.com/news/2019/08/open-source-photo-video-matching/

52 See: https://news.microsoft.com/2009/12/15/new-technology-fights-child-porn-by-tracking-its-photodna/

"A lot of the voluntary work around detection of CSAM is based on these databases, and happening in a relatively limited way. However, the technology that's being deployed to do that is already being deployed also to look for terrorist content. It's even potentially being deployed to look for misinformation and disinformation."[53]

There is less information in the public domain about the technology that operates in live and real-time digital environments. A 2021 Council of Europe independent experts report[54] stated that Microsoft has been leveraging tools for the purposes of detecting grooming, built on artificial intelligence (AI) and aimed at targeting behaviours in programs on their Xbox platform for several years and was exploring its use in chat services, including Skype. However, that may now be out of date,[55] as the terms and conditions at the time of writing state[56] that, "we do not monitor the Services and make no attempt to do so."

The hopes of some people who support victims and survivors we spoke to, rest on further emerging technologies that will grant access to live conversations and behaviours to a wider range of people such as safeguarding professionals, including for example the UK project DRAGON-S, (Developing Resistance Against Grooming Online – Spot and Shield). The proposal to triage conversations that human operators believe should be inspected in more detail will still need to respect human rights principles like necessity and proportionality.[57]

One area of risk and harm that deserves attention in the context of the broader child protection system is identifying images that are consensual peer-to-peer indecent image sharing, commonly known as "sexting". The child's actions constitute a criminal offence in the UK and many other jurisdictions, but the intent of most adults supporting young people is to not criminalise them and formal sanction against a child or young person would be considered exceptional.[58]

53 CRIN and ddm interview with Privacy International, 26 September 2022.

54 Council of Europe, *Independent Experts' Report: Respecting human rights and the rule of law when using automated technology to detect online child sexual exploitation and abuse*, 2021, p. 24, https://rm.coe.int/respecting-human-rights-and-the-rule-of-law-when-using-automated-techn/1680a2f5ee

55 See: https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/

56 See Microsoft Services Agreement from August 2022: https://web.archive.org/web/20221204112549/https://www.microsoft.com/en-gb/servicesagreement

57 This platform has been collaboratively developed with Legal Innovation Lab Wales, supported by the European Regional Development Fund through the Welsh Government: https://www.swansea.ac.uk/project-dragon-s/

58 See CRIN, *Discrimination and Disenfranchisement: A global report on status offences*, 2016, pp. 38-41, https://archive.crin.org/sites/default/files/crin_status_offences_global_report_0.pdf; See also: https://childlawadvice.org.uk/information-pages/sexting/

Workarounds for encryption and exploits in security in the context of child protection

The difficulties posed in identifying illegal behaviour in end-to-end encrypted environments, including child sexual abuse and exploitation, have led to a number of proposals for how to overcome this challenge.

Client-side scanning

Client-side scanning is a means of monitoring the content and behavioural data generated on a device, as opposed to in transit. This means that outgoing communication from a device is scanned and checked against a list of known images or words before it is sent. If there is a match, the system can refuse to send the message or may report it to law enforcement or watchdog organisations. Client side scanning has been proposed in particular as a means of identifying child sexual abuse material that is shared across encrypted channels by scanning messages before they are encrypted and sent, but there is nothing about the technique or technology that limits it to identifying any particular type of image or content.

There are also similar "hybrid" style scanning measures, such as those proposed by Apple in 2021. Facing criticism, the company decided to change some of its plans and pause others,[59] but the proposals were that where users were backing up photos by copying them to Apple servers, this would initiate a scanning process. This method of detecting child sexual abuse material is not strictly "client-side" but a "hybrid on-device/server pipeline". While the first phase of the hash matching process[60] runs on the device, its output is only interpreted through the second phase, run on Apple's iCloud Photos servers. Apple announced a change of its plans in December 2022 to refocus its efforts on growing its Communication Safety feature.[61]

The intended plan was that if already known child sexual abuse images were uploaded to Apple's iCloud servers in the number that exceeded the review threshold, Apple would detect a match in a database of hashes of images provided by the National Center for Missing and Exploited Children. Although the system uses machine learning to detect minor alterations, for example if the images were cropped, or compressed differently, it would not detect an unknown image.

Several experts interviewed during research for this report saw advantages to

59 EFF, *Apple Has Listened And Will Retract Some Harmful Phone-Scanning*, 12 November 2021, https://www.eff.org/deeplinks/2021/11/apple-has-listened-and-will-retract-some-harmful-phone-scanning

60 Apple, *Security Threat Model Review of Apple's Child Safety Features*, August 2021, https://www.apple.com/child-safety/pdf/Security_Threat_Model_Review_of_Apple_Child_Safety_Features.pdf

61 CNN Business, *Apple abandons controversial plan to check iOS devices and iCloud photos for child abuse imagery*, 8 December 2022, https://edition.cnn.com/2022/12/08/tech/apple-csam-tool/index.html

the use of client-side scanning as a less intrusive means of identifying content transferred through encrypted channels, since the technology does not seek to have access to the entirety of the user's communications, but operates before the encryption or after the decryption of the communications, and it does not actually "read" the messages:

> *"One myth is the idea of looking at pictures or scanning your photos. That's not what happens. [...] They're 1s and 0s. No one's looking at anything. It'll just be a string of numbers compared to another string of numbers. And if they match, take action."*[62]

However, many people and organisations who work with technology are concerned about proposals that support client-side scanning because any access for people who were not intended to be part of a particular communication requires a way in. Any "back-door" access "increases the 'attack surface' for encrypted communications by creating additional ways to interfere with communications by manipulating the database of prohibited content", and it can't be guaranteed to be accessed by only "the good guys" according to the Internet Society in their response to the leaked 2020 working copy of an EU Commission paper.[63]

Fourteen experts in computer science, including from Cambridge University and the Royal Society to MIT and a fellow of the IEEE, the authors of the paper *Bugs in our Pockets: The Risks of Client-Side Scanning* (2021) remain unconvinced and believe that the promise of client-side scanning is an illusion.

They explain that, "moving content scanning capabilities from the server to the client opens new vantage points for the adversary", and argue that if the client-side scanning technologies and practice were to become pervasive, there would be "an enormous incentive for nation-states to subvert the organisations that curated the target list, especially if this list were secret".

Similar criticism has been made that client-side scanning breaks end-to-end encryption in principle if not in practice by creating the route for interference by a third-party, because "fundamentally it's very targeted at finding the content of the end-to-end encrypted communication: understanding what's about to be sent, or what has been sent and received on the device itself. So that breaks the expectation that this is supposed to be a private communication only between the known participants. And more broadly, it is likely to be incredibly disproportionate because of the ability to scan for all types of content and potentially heavily censor that content - not only indicate that certain content is about to be sent or has been sent, but also potentially even block that content from being sent."[64]
Critics of the use of the measure have also raised concerns about the risk of

62 CRIN and ddm interview with IWF, 3 November 2022.

63 Leaked EU Commission working document: *Technical solutions to detect child sexual abuse in end-to-end encrypted communications*, 2020, https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf

64 CRIN and ddm interview with Privacy International, 26 September 2022.

"mission creep", whereby measures are introduced exclusively to identify child sexual abuse images, but are then expanded in a way that leads to much greater intrusion and reporting of individuals activities - legal or otherwise - to authorities. Researchers at Princeton in 2021, stopped their own scanning program when they realised how easily their system could be repurposed for surveillance and censorship. "The design wasn't restricted to a specific category of content; a service could simply swap in any content-matching database, and the person using that service would be none the wiser."[65] That China and India have repurposed such technology for these aims,[66] makes this a very real not theoretical risk.

Some proposals to implement scanning the device respond in some respects to this concern, warning the user when a match is identified and blocking the content, but not notifying the authorities. Even in this case, some interviewees were wary of mission creep: "If people are used to a system like that on their phone running in the background, then how hard would it be to flip the switch and start reporting back to the authorities? [...] It's such a powerful tool and many governments around the world that are more repressive are going to want to have access to it and expand it beyond [child sexual abuse material]."[67]

> *"From a policy perspective you could try to put controls and limits in place, but of course the next government might have different views and get rid of those controls. [...] Once the tech is in place, people will come up with all sorts of ideas about how this technology could be used to deal with new societal problems. [...] [It has been widely said that] 'Code is law', that technology has legal impact. I actually think it goes further than that. I think in some ways technology is like constitutional law, where it puts things in place that are very difficult to change later. Once every iPhone and every Android has this kind of CSAM scanning capability, well, why shouldn't governments ask it to start looking for bomb-making instruction manuals, extremist images, and insults to religious figures?"*[68]

Dr Ian Levy, former Technical Director of the National Cyber Security Centre (NCSC) and Crispin Robinson, Technical Director for Cryptanalysis at GCHQ, promoted a more overt client-side scanning approach in their July 2022 paper as a way of achieving the same aim in mass surveillance and claim it does so without endangering user privacy. Others disagree. Because this privacy interference is performed at the scale of entire populations, a group of leading security and encryption experts describe it as a bulk surveillance technology in their paper "Bugs in our Pockets", published in the summer of 2021.[69] They explained why it

65 9to5Mac, *Princeton University says it knows Apple's CSAM system is dangerous – because it built one*, 20 August 2021, https://9to5mac.com/2021/08/20/apples-csam-system-is-dangerous/

66 EFF, *India's Draconian Rules for Internet Platforms Threaten User Privacy and Undermine Encryption*, 20 July 2021, https://www.eff.org/deeplinks/2021/07/indias-draconian-rules-internet-platforms-threaten-user-privacy-and-undermine

67 CRIN and ddm interview with Privacy International, 26 September 2022.

68 CRIN and ddm interview with Ian Brown, 6 October 2022.

69 Abelson, H. et al., *Bugs in our Pockets: The Risks of Client-Side Scanning*, 2021, https://arxiv.org/

makes what was formerly private on a user's device potentially available to law enforcement and intelligence agencies, even in the absence of a warrant.

> *"[Client-side-scanning] neither guarantees efficacious crime prevention nor prevents surveillance. Indeed, the effect is the opposite. CSS by its nature creates serious security and privacy risks for all society while the assistance it can provide for law enforcement is at best problematic. There are multiple ways in which client-side scanning can fail, can be evaded, and can be abused."*

This risk of scope creep creates the very real question of what limits the technology from becoming an all-purpose facial recognition and reporting tool for the state? Since some aspects of proposed legislation in the EU would make reporting mandatory, and in the US the reporting of child sexual abuse material to NCMEC is already mandatory,[70] the question arises of whether organisations involved in monitoring reporting, such as NCMEC are wholly private or in the legal context, a "state actor." This question in turn raises questions about appropriate scrutiny and oversight.

In the August 2022 Report, *The right to privacy in the digital age*, the Office of the UN High Commissioner for Human Rights made several comments around Client-Side Scanning, namely that:

> *"Client-side scanning also opens up new security challenges, making security breaches more likely."*[71]

> *"Imposing general client-side scanning would constitute a paradigm shift that raises a host of serious problems with potentially dire consequences for the enjoyment of the right to privacy and other rights. Unlike other interventions, mandating general client-side scanning would inevitably affect everyone using modern means of communication, not only people involved in crime and serious security threats."*[72]

> *"Given the possibility of such impacts, indiscriminate surveillance is likely to have a significant chilling effect on free expression and association, with people limiting the ways they communicate and interact with others and engaging in self-censorship."*[73]

pdf/2110.07450.pdf

70 Rosenzweig, *The Law and Policy of Client-Side Scanning*, 20 August 2020, https://www.lawfareblog.com/law-and-policy-client-side-scanning

71 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/51/17, 4 August 2022, para. 28, https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age

72 Id., para. 27.

73 Ibid.

Homomorphic encryption and emerging technologies

On-device homomorphic encryption - a form of encryption which allows users to carry out computations on encrypted data without decrypting it - with server-side hashing and matching has been suggested as a technology with potential. Using this method, images are encrypted using a carefully chosen partially homomorphic encryption scheme, which enables an encrypted version of the hash to be computed from the encrypted image. The encrypted images are sent to the online service provider server for hashing and matching against an encrypted version of the hash list. The server does not have the homomorphic encryption keys so cannot access the contents of the image, but can only identify if there is a match or not in the database of images. If the database contains only one kind of image content the server provider can therefore infer what was identified as on the users' device but not access the image itself.

Some interviewees thought that investing in privacy-enhancing technologies like homomorphic encryption would be a way to move the debate forward.

> *"We've had conversations with industry partners and said, 'Have you been looking at this?', but one of the comments that came back was 'It's too expensive'. [...] But actually that would be a really positive way of using encryption. I can match something without ever knowing what I'm matching and what I'm actually matching it against. [...] It's a way of using an encryption method to expose as little information as possible."*[74]

> *"My general perception is of technology that just keeps getting better and faster. [...] There have been theoretical conversations about homomorphic encryption or quantum computing and how it may lead to the ability to break encryption, but I think we're just so far away from those solutions. And by the time we get to that point, we'll have much more powerful encryption, too."*[75]

However, easier access to systems, networks and devices, all increases risk of misuse that the European Union Agency for Cybersecurity (ENISA)[76] sees cannot be fought with technology.

Research by Tech Against Terrorism found that the technology is not yet fully developed, and developing such solutions is expensive. Further, it presents security risks, raises jurisdictional questions, and breaches privacy.[77]

74 CRIN and ddm interview with IWF, 3 November 2022.

75 CRIN and ddm interview with Privacy International, 26 September 2022.

76 ENISA, *Solving the Cryptography Riddle: Post-quantum Computing & Crypto-assets Blockchain Puzzles*, 2021, https://www.enisa.europa.eu/news/enisa-news/solving-the-cryptography-riddle-post-quantum-computing-crypto-assets-blockchain-puzzles

77 Tech Against Terrorism, *Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies*, 2021, p. 62.

The UK Information Commissioner's Office describes how important it is to choose the right algorithm, and to ensure that the key size is large enough to defend against attack over the full life-cycle of the data.[78] As computing processing power increases or new mathematical attack methods are discovered, a key must remain sufficiently large to ensure that an attack remains a practical impossibility. Quantum computing creates new risks for every previous form of cryptography.

According to ENISA, quantum technology will, "enable a huge leap forward in many branches of industry, as it can efficiently resolve problems technologies of today are not able to provide a solution for. However, this technology will be highly disruptive for our current security equipment and systems. Scientists commonly agree that quantum computers will be able to break widely used public-key cryptographic schemes."[79]

Covert access to live content via wiretapping

Another approach to accessing data that is encrypted is through covert monitoring. Various terms are used interchangeably to describe this kind of activity, including "lawful exceptional access" and "legal hacking", but the most well known proposal was the so-called "ghost protocol". What all of these measures have in common is that they seek to gain covert access to encrypted communications.

The "ghost protocol",[80] from GCHQ proposed adding a silent third-party to encrypted conversations. In its simplest terms, this would mean that law enforcement or national security actors would be able to access content discussed in encrypted environments, without undermining the encryption itself as they would be part of the conversation. The measure has been widely condemned by technology and privacy groups, including the Internet Society.[81] "While optimism and cooperation are nice in principle, it seems unlikely that communication providers are going to *voluntarily* insert a powerful eavesdropping capability into their encrypted services, if only because it represents a huge and risky modification."[82]

78 UK Information Commissioner's Office, *Encryption*, 2022, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/#new

79 ENISA, *Solving the Cryptography Riddle: Post-quantum Computing & Crypto-assets Blockchain Puzzles*, 2021.

80 Levy, I. and Robinson, C., *Principles for a More Informed Exceptional Access Debate*, 2018.

81 Internet Society (ISOC), *Ghost Protocol Fact Sheet*, 2020.

82 Ibid.

> *"It has been said that the ghost proposal does not break encryption - it does not require the removal of encryption because you're just adding a silent invisible user. [...] But from our perspective, that creates a huge security vulnerability. [...] This ghost is obviously intended to be law enforcement, but [...] criminals might be able to get access to that technology, states that don't respect human rights might force service providers to use it to gain access to encrypted communications without the knowledge of the participants, and ultimately that breaks encryption."*[83]

"Legal hacking" presents another means of gaining access to encrypted environments. These measures try to exploit security vulnerabilities to gain access to end-to-end encrypted communications, whether by intentionally creating a weakness that authorities know how to access or taking advantage of an unintended defect in the security.

> *"Ultimately what they have in common is that they either mandate or try to exploit vulnerabilities. So to my mind they undermine the very essence of encryption, which is that no person can have access to the communication other than the sender and the receiver. So it's essentially creating a vulnerability in the system which then law enforcement are able to have access to. Now, that's kind of like building a house and saying you can have a lock on the front door, but you need to have a back door that the police can enter when they have a court order and all that really does is it creates an opportunity for someone else to break in."*[84]

Some interviewees argued that legal hacking should be acceptable if it complies with extremely stringent safeguards, for example ensuring that it does not undermine the security of the device as a whole. In any case, as one interviewee put it, "Governments already gain access to encrypted communications content by launching brute force attacks or employing other technical means to circumvent encryption. Such measures need to be regulated, and cabined with procedural and substantive safeguards governing such access on a case-by-case basis".[85]

83 CRIN and ddm interview with Privacy International, 26 September 2022.

84 CRIN and ddm interview with Richard Wingfield, 6 September 2022.

85 CRIN and ddm interview with the Centre for Democracy and Technology (Europe Office), 13 October 2022.

Other commentators have been more sceptical about the possibility of achieving this kind of access safely without fundamentally undermining encrypted communications:

> *"We know that hackers and those who would want to access people's encrypted communications are as technologically savvy and in often cases more so than security and law enforcement agencies, so it would only be a matter of time before any vulnerability that was mandated became identified by others, so you'd constantly be playing a cat-and-mouse game of fixing a vulnerability and then having to create a new one. So I don't think that ultimately that's a sustainable solution. You might as well not have encryption in the first place if you're going to have a vulnerability in that case."*[86]

In practice, law enforcement have a number of tools at their disposal that function as "lawful hacking". GrayKey enables law enforcement to recover data from iOS and leading Android devices, including encrypted or inaccessible data. Cellebrite's Universal Forensic Extraction Device, software that extracts the data from a mobile phone and generates a report summarising it, can even detect and report on deleted data. Other tools are IMSI catchers, essentially a "fake" mobile tower acting between the target mobile phone and the service provider's real towers, which are considered a man-in-the-middle (MITM) attack. These high-cost technology solutions are increasingly procured and used by States. Where States have found these measures politically unpalatable or legally not possible, some are ignoring the principles of the rule of law, democracy and human rights and instead procure other third-party services to do the spying on their behalf.[87]

Researchers found in Nigeria that the government has increased spending in the last decade on acquiring various surveillance technologies and has approved a supplementary budget to purchase tools capable of monitoring encrypted WhatsApp communications.[88]

86 CRIN and ddm interview with Richard Wingfield, 6 September 2022.

87 For example, the Israeli NSO Group's Pegasus spyware, which was implicated in the murder of Saudi journalist Jamal Khashoggi.

88 Oloyede, R. and Robinson, S., *Surveillance laws are failing to protect privacy rights: What we found in six African countries*, 26 October 2021, Institute of Development Studies, https://www.ids.ac.uk/opinions/surveillance-laws-are-failing-to-protect-privacy-rights-what-we-found-in-six-african-countries/; Premium Times, *Nigerian govt moves to control media, allocates N4.8bn to monitor WhatsApp, phone calls*, 12 July 2021, https://www.premiumtimesng.com/news/headlines/473147-as-nigeria-moves-to-control-media-nia-gets-n4-8bn-to-monitor-whatsapp-phone-calls.html

Covert access to live content via malware and interception

Access to encrypted communications can also be achieved through installing "malware" (malicious software) on a device to allow access. The most high profile example of this has been the use of "Pegasus", software developed by the NSO Group. The software can be installed on a phone remotely without the owner knowing and turns it into a surveillance device. The software can copy messages that are sent or received, access photos, turn on the microphone to record conversations, turn on the camera and access location data.

Research by the Citizen Lab in 2020, found what they called "a bleak picture of the human rights risks of NSO's global proliferation". Countries with significant Pegasus spyware operations had previously been linked to abusive use of spyware to target civil society, including Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia, and the United Arab Emirates. In August 2016, the award-winning UAE activist Ahmed Mansoor was targeted with NSO Group's Pegasus spyware.[89]

Whether on request, or through approved "lawful interference" or by indirect government interference through hacking,[90] as soon as it is possible to open up the contents of communications to a company, by extension the government and law enforcement have access in ways that they wouldn't otherwise have.

These threats are supplementary to insider threats. In 2019, the US Department for Justice charged two former Twitter employees with accessing the personal information of more than 6,000 Twitter accounts in 2015 on behalf of Saudi Arabia.[91] Secure enclave technology, which are in effect "secure settings" inside businesses where not all employees have all access, are designed to mitigate but cannot solve this problem.

There is a lack of trust in governments around the world to not misuse the communications data of their opponents in many shapes and forms. Individuals rely on universal fundamental human rights in law as a deterrent and as a route for redress, where they cannot rely on a government to be trustworthy.

89 Marczak, B. et al., *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, 2018, Citizen Lab Research Report No. 113, University of Toronto, https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf

90 UK Government, *National Cyber Force Transforms country's cyber capabilities to protect UK*, 19 November 2020, https://www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk

91 Washington Post, *Former Twitter employees charged with spying for Saudi Arabia by digging into the accounts of kingdom critics*, 6 November 2019, https://www.washingtonpost.com/national-security/former-twitter-employees-charged-with-spying-for-saudi-arabia-by-digging-into-the-accounts-of-kingdom-critics/2019/11/06/2e9593da-00a0-11ea-8bab-0fc209e065a8_story.html

Breaking encryption myths

"Breaking" encryption for data in transit, the content of communications, involves being able to read the contents "in the clear" and joined up the way the sender intended for the recipient to read. That means either you obtain the key by being given, finding, guessing or compelling it from the sender, or you bypass the key by exploiting a flaw, to access the plain contents in use or locate a copy of it. Which method is used depends on who is looking for what access to what content and why. The EU assessment of effectiveness feasibility and risks and outcomes of various workarounds can be read in a leaked 2020 working copy of an EU Commission paper.[92]

As more and more content has been made secure in-transit and with increasing use of peer-to-peer systems, the points at which any third-party can most easily access communications data is at the end points. The debate around end-to-end encryption has therefore become more fraught as time has gone on, as security services, states, and law enforcement suggest more effective security for users makes it harder for security services to break into them. The push therefore is towards services that do not need to "break encryption" where it is used and instead to operate on the device, or server that is the end-point of the process. While these techniques may therefore not compromise the technical architecture of end-to-end encrypted systems as a whole, they compromise its purpose and aims in practice.

Generally the concept of "breaking encryption" in the context of detection and enforcement of law enforcement for child protection, has been superseded by the widespread use of an alternative approach: the encryption workaround.[93] The technology does not need itself to be broken if the achievement of the aims of the end-to-end encryption can be broken instead.

User reporting

Effective user reporting is widely recognised as a vital part of any policy and practice, whether by company to bodies responsible for identification and takedown or at individual levels.

For example, WhatsApp reports all apparent instances of child exploitation appearing on their service from anywhere in the world to NCMEC, according to their published policy,[94] including via government requests.

92 Leaked EU Commission working document: *Technical solutions to detect child sexual abuse in end-to-end encrypted communications*, 2020.

93 Kerr, O. S. and Schneier, B., *Encryption Workarounds*, 2017, 106 Georgetown Law Journal 989 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033

94 See: https://faq.whatsapp.com/444002211197967/?locale=lv_LV

> *"I think user reporting is actually something that should be encouraged as much as possible, assuming that what's being reported is legitimately illegal behaviour or material. [...] Regulation is needed to make it easier for users to be able to report material and behaviour that violates platforms' terms of service and to have a clearer and more transparent process by which that assessment is then made by the company, and then look into appeal mechanisms etc. It should be as easy as possible, particularly for children and other vulnerable users, to report something potentially harmful, and to understand the rules of the platforms they use to be able to report harmful or illegal activity and behaviour by other people. [...] Children should be better equipped, as they are growing up using technologies, to know how to use them safely and securely, whether that's through schools, or by initiatives of the platforms or design choices by the platforms themselves."*[95]

User reporting by individuals and organised collectives may of course be used against individuals in unexpected ways or weaponised at scale as well.

WhatsApp users have used the reporting system to attack other users according to moderators interviewed by ProPublica, who said in 2021, "we had a couple of months where AI was banning groups left and right" because users in Brazil and Mexico would change the name of a messaging group to something problematic and then report the message. "At the worst of it," recalled the moderator, "we were probably getting tens of thousands of those. They figured out some words that the algorithm did not like."[96]

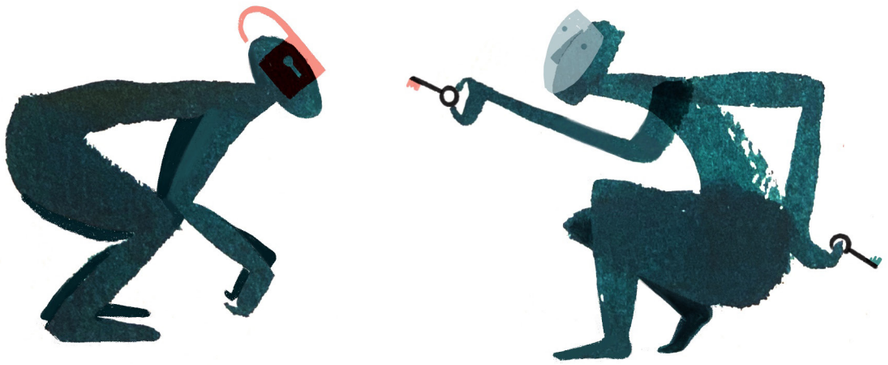
However, user reporting is the one approach that does not create tensions with privacy and security in encrypted environments, with little to no technical challenge. Interviewees, especially those involved in victim and survivor support, frequently highlighted that user reporting was inadequately supported, and took too long, sometimes with weeks in between, from reporting to takedown. That will likely become increasingly politically and publicly unacceptable with mounting pressure on social media companies from new legislation around the world.

95 CRIN and ddm interview with Richard Wingfield, 6 September 2022.

96 Ars Technica, *WhatsApp "end-to-end encrypted" messages aren't that private after all*, 8 September 2021, https://arstechnica.com/gadgets/2021/09/whatsapp-end-to-end-encrypted-messages-arent-that-private-after-all/

Summary: Technology discussed in debate around combatting child violence and sexual exploitation

		E2EE in transit with content hash extraction and matching is at point of upload to the service provider or on providers' servers			Workarounds of encryption or exploits in security						
	Photo DNA (only operates in unencrypted environments e.g. websites without https and non-e2ee messaging, and at points where the content is unencrypted at rest i.e. at the service provider or on device).	On-device homomorphic encryption with server-side image hashing and matching (i.e. Apple 2022)	Text based scanning tools (only operates in unencrypted environments e.g. in the open web and unencrypted points in communications channels)	On-device client-side detection with cloud-based second stage image or text based moderation	Secure enclaves in the service provider's server with matching via homomorphic encryption	On-device overt access with information sent to another device (e.g. "parental control" style products)	Key Escrow chips installed in the device at mass scale (e.g. The Clipper Chip)	Spyware (remote covert access to a mobile device not authorised by the device owner e.g. Pegasus)	On-device hacking (physical device access not unauthorised by the device owner e.g. Cellebrite)	Server-side access to all content by design (e.g. man-in-the-middle style tools including "Child Safety Tech" products)	Ghost protocol (adding a third party to a communication while in progress unknown to the device owner e.g. state intelligence services)
Characteristics of the tools											
Targeted only at individuals (can also be employed at scale)						X		X	X		X
Untargeted	X	X	X	X	X		X		X	X	
Identifies content in an encrypted environment		X		X	X	X	X	X			X
Enables mass surveillance of content by companies	X	X	X	X	X		X	X		X	X
Enables mass surveillance of content by law enforcement / security services	X	X	X	X	X		X	X		X	X
State security services exceptional access possible (its legality depends on jurisdiction)	X	X	X	X	X	X	X	X	X	X	X
Compliant with a ban on general monitoring											
Application of the tools											
Previously identified (recirculating) CSAM images children aged under 13	X	X		X	X	X	X	X	X	X	X
Previously identified (recirculating) CSAM images children aged aged 13-18	X			X	X	X	X	X	X	X	X
Previously unknown CSAM images of children aged under 13				X		X	X	X	X	X	X
Previously unknown CSAM images of children aged 13-18				X		X	X	X	X	X	X
Real-time grooming via camera (video)			X	X		X	X	X	X	X	X
Real-time sextortion via camera (video)			X	X		X	X	X	X	X	X
Illegal content exchanged in e2ee messaging between adult and child (text or image based)			X	X	X	X	X	X	X	X	X



Frictions and faultlines: The search for consensus

"There is a lot more common ground in the debate than perhaps some of us recognise. [...] It's the details where it gets tricky."[97]

The encryption debate was once described as "thermonuclear", with "emotions running high on either side".[98] To move beyond the divides that currently exist with regard to encryption, it is necessary to understand the frictions, fractures and faultlines that exist in this space as well as where there is room for consensus.

This chapter explores the themes that emerged throughout the interviews, private conversations and literature review that form the backbone of this report, with a view to better understanding the perspectives and thinking regarding children's rights and encryption and identifying a way forward.

The pressing need to address online child sexual abuse and exploitation

The discussion about the proper regulation of encryption and the challenges of preventing and identifying online child sexual abuse and exploitation have become inextricably linked. Particularly in the European and North American context, this issue occupies a central point in legislative and regulatory reform processes. It is also in this context that many of the most explicit tensions emerge. Yet despite these tensions, across the full range of interviews, conversations and literature reviewed as part of this research, there was no dispute that online child sexual abuse and exploitation requires urgent action to protect children and secure the accountability of abusers. Where disagreement was evident, it related to the different perspectives on how to achieve this goal and how to protect human rights more broadly in doing so.

> *"It's not a question of: should we protect children or not? We completely agree on the need for protection."*[99]

> *"We all want to protect children. [...] The point is that the means of doing so can be different."*[100]

---

97 CRIN and ddm interview with WeProtect Global Alliance, 19 August 2022.

98 POLITICO, *Europe's thermonuclear debate on privacy and child sexual abuse*, 20 November 2020, https://www.politico.eu/article/europes-thermonuclear-debate-on-privacy-and-child-sexual-abuse-2/

99 CRIN and ddm interview with Electronic Frontier Norway, 15 September 2022.

100 CRIN and ddm interview with ISOC, 30 August 2022.

Despite this fundamental basis of agreement, many interviewees who reflected on the public debate about encryption and online child sexual exploitation and abuse described an environment that had become hostile and emotive in a way that has held back reform. Some participants revealed that during conversations on the risks of encryption – particularly in the context of child abuse – they witnessed a tendency to move away from the criticism of arguments towards more personal denunciations of what were perceived to be callous, immoral positions. As one interviewee pointed out, "rarely do we get the chance to have a nuanced informed debate around this because it's just so emotional".[101] Others identified instances of "scaremongering" and "rhetoric" that is quite inflammatory, sometimes even toxic, in the debate.

This tension risks preventing the engagement across different areas of expertise that will be necessary to meaningfully address online child sexual abuse and exploitation. Yet despite this challenge, interviewees commonly felt that the conversation was now shifting to make progress possible. In the words of one interviewee: "It does feel like ground has been conceded on both sides. I feel kind of quietly optimistic about getting to a place where there's more understanding on both sides."[102]

A note on the scale of online child sexual abuse and exploitation

"Numbers just look very flat when there's a much more robust story behind them."[103]

"What's an acceptable number of children being sexually abused? I just don't think that's ever a question we should be asking ourselves."[104]

In 2021, NCMEC received 29.3 million reports of suspected child sexual exploitation, 35 per cent more than in 2020. The reports provided by electronic service providers included 39.9 million images, of which 16.9 million images were unique, and 44.8 million videos, of which 5.1 million were unique.[105]

Given the prominence of the principles of necessity and proportionality in the debate on encryption and children's rights, there is a tendency to reach for numbers in order to advocate for particular solutions.

The data has been seen as "vital to enabling nations to understand the extent" of the problem of child sexual abuse material online and to making the case for "increased government investment" in tackling it.[106] The data has also been used in arguing about the effectiveness and necessity of automated detection tools, and in warning about the consequences of turning them off.[107] For example, NCMEC saw a 58 per cent decrease in reports of EU-related child sexual exploitation when the EU ePrivacy Directive went into effect and before the temporary derogation was adopted,[108] which limited industry's ability to detect, report and remove child sexual abuse material.[109]

However, numbers are not as helpful in moving the debate forward as it may seem. Some fear that at times "people might glaze over numbers that feel just too large to think about".[110] In any case, the current numbers are far from accurate depictions of the problem. As one interviewee from NCMEC explained, underreporting is felt to be a significant issue, because platforms fear the reputational risks of making a large number of reports: "there are many companies out there that are maybe in everyone's pockets or everyone's purse right now, and they have very few reports, and we just know that this is not a reflection of what is happening on their services".[111] The emerging trend of "sextortion", a "combination of white collar crime and child sexual exploitation"[112] also complicates the picture, because digital payment platforms over which the exchange between the abuser and the child happens do not report financial activity as sexual abuse.

On the other hand, the data is sometimes felt not to be a true reflection of the nature and extent of the problem because of the number of duplicate pieces of content in circulation. For instance, a study carried out by Meta on content reported to NCMEC in October and November 2020 revealed that "90% of this content was the same as or visually similar to previously reported content. And copies of just six videos were responsible for more than half of the child exploitative content we reported in that time period", indicating that "the

101 CRIN and ddm interview with 5Rights, 5 September 2022.

102 Ibid.

103 CRIN and ddm interview with NCMEC, 3 November 2022.

104 CRIN and ddm interview with IWF, 3 November 2022.

105 NCMEC, *CyberTipline 2021 Report*, https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

106 Kardefelt-Winther, D. et al., *Encryption, Privacy and Children's Right to Protection from Harm*, 2020, UNICEF Office of Research – Innocenti Working Paper 2020-14, p. 9, https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf

107 Dan Sexton (IWF), *Not all Encryption is the same: social media is not ready for End-to-End Encryption*, 14 March 2022, https://www.iwf.org.uk/news-media/blogs/not-all-encryption-is-the-same-social-media-is-not-ready-for-end-to-end-encryption/

108 See the chapter on recent legislative proposals.

109 NCMEC, *Battle won but not the war in the global fight for child safety*, 11 May 2022, https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety

110 CRIN and ddm interview with NCMEC, 3 November 2022.

111 Ibid.

112 Ibid.

number of pieces of content does not equal the number of victims, and that the same content, potentially slightly altered, is being shared repeatedly".[113]

To these points survivors and child protection advocates responded forcefully: "People are assuming that that's a good thing, because fewer images are being shared more times. But that doesn't offer me any comfort. So if my image is shared one time, that's horrific. If my image is being shared 1,000 times or 10,000 times… am I supposed to feel better because it's the same image?",[114] and "There's something kind of disingenuous in saying it's repetitive. It's not. It's a new crime every single time, with a new perpetrator and a new victimisation. It's like the humanity is lost in this conversation, right?"[115]

If some numbers must be sought, perhaps what is more important than the amount of total reports is the number of "meaningful reports",[116] which provide information that could potentially save a child. But, according to the interview with NCMEC, too many companies provide instead "barely a shell of a report"[117] in what seems like a tick-boxing exercise.

Even where there is some agreement on the importance of numbers and what they mean, it is not clear to what extent reports lead to actually solving crimes against children. Regarding the UK specifically, the National Crime Agency "received 102,842 reports from NCMEC, but some of these were incomplete or, once investigated, not found to be child abuse. Of these, 20,038 [reports] were referred to local police forces and started (or contributed to) investigations. In the same year, over 6,500 individuals were arrested or made voluntary attendances due to offences related to child abuse and over 8,700 children were safeguarded."[118] But the response from national law enforcement "varies widely as a consequence of capacity and resource constraints". It is far from clear "how many investigations and arrests directly derive from NCMEC reports at the global level, or how many fewer would have been made with end-to-end encryption implemented".[119]

113 Meta, *Preventing Child Exploitation on Our Apps*, 23 February 2021, https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/

114 CRIN and ddm interview with the Marie Collins Foundation, 22 November 2022.

115 CRIN and ddm interview with NCMEC, 3 November 2022.

116 Ibid.

117 Ibid.

118 Levy, I. and Robinson, C., *Thoughts on child safety on commodity platforms*, 2022, p. 3.

119 Kardefelt-Winther, D. et al., *Encryption, Privacy and Children's Right to Protection from Harm*, 2020, UNICEF Office of Research – Innocenti Working Paper 2020-14, p. 9.

Privacy and protection

"Really the challenge that we have here is: how do we safeguard children, whilst protecting privacy and other fundamental rights?"[120]

"We need to have a balanced conversation about all of the rights that takes into account safety as well as privacy."[121]

A second, central point around which debate has formed has been the characterisation of online regulation as a matter of "privacy versus protection", or sometimes more bluntly "protection of children versus privacy of adults". This divide, often seen as at the core of disputes with regards to encryption, did sometimes appear in advocacy messaging reviewed during the research for this report, but among the interviewees and more in depth written analysis, issues related to privacy and encryption were rarely treated in those terms.

As might be expected, the defence of the value of privacy in the regulation of encryption was strongly made among organisations and experts whose work focuses on privacy, as well as those working most directly with technology. As one interviewee put it, "We fight to protect privacy because we know that it's a really important right and in many ways a gatekeeper to other rights. [...] Under surveillance, people are suppressed and their rights are limited [...] Privacy is a fundamental underpinning of how states work and violations to privacy are very, very concrete and can lead to huge harms. [...] We know from history how dangerous it is when our privacy is intruded on by the state - having the right to privacy is about redressing that balance of power."[122]

This perspective, however, was not limited to organisations focused exclusively on privacy rights. Some children's rights advocates stressed that, both in the debate around encryption and more generally, privacy is often wrongly seen as the preserve of adults. They viewed this as a symptom of a general failing in the way that children's rights are discussed, which tends to regard children as "objects of protection instead of fully formed subjects of rights".[123]

The same interviewee emphasised that children have the right to privacy, but also added that there needs to be a better understanding of how privacy impacts their development.[124] One interviewee warned that "if privacy is violated, especially

120 CRIN and ddm interview with EDRi, 9 August 2022.

121 CRIN and ddm interview with IWF, 3 November 2022.

122 CRIN and ddm interview with EDRi, 9 August 2022.

123 CRIN and ddm interview with the Alana Institute, 22 September 2022.

124 See, for example, the idea that Art. 8 of the European Convention on Human Rights protects the right to personal development, whether in terms of personality or of personal autonomy: European Court of Human Rights (Registry), *Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence*, updated on 31 August 2022, p. 25, https://www.echr.coe.int/documents/guide_art_8_eng.pdf

during childhood, when key aspects of psychological and emotional life are being developed, this can jeopardise the formation of social and political individuals."[125] Another echoed this concern, stating that "children who are being surveilled feel that they cannot actually express themselves freely, in an independent way. And this might actually affect their development and the way they put their personalities out there in the world."[126]

> *"[Privacy] allows children to safely develop their personality, to find out who they are."*[127]

Many interviewees emphasised that privacy enables the exercise of other rights, including protection from violence, strongly supporting the idea that privacy has a protection element to it. This protective element was particularly stressed in so far as it relates to children from disadvantaged and marginalised groups. Interviewees pointed to the link made between privacy and safety in General Comment No. 25 of the UN Committee on the Rights of the Child, which states that "privacy is vital to children's safety".[128]

Digital privacy advocates also suggested that the "privacy versus protection" polarisation might be partly due to "a perception that privacy is somehow abstract and hypothetical, getting in the way of the concrete right to protection of children".[129] They were concerned by the suggestion that those who have nothing to hide should not fear the weakening of encryption. To this perception they forcefully responded that a preference for encrypting communications to keep them private does not in and of itself indicate any harmful activity. Overall, they strongly emphasised the importance of privacy as a fundamental right which is not inferior or secondary to protection.

Among the most contentious applications of children's right to privacy that emerged from this research was in relation to that of survivors of child sexual abuse. A number of child protection advocates argued that there tends to be a one-sided view of privacy in the debate around encryption, that treats encryption as wholly positive in terms of promoting privacy. They felt that too little attention is paid to the way encryption threatens the privacy of those who have been sexually abused: "What about the rights of victims whose images are being spread using encrypted channels? What about survivors who know that their images have been repeatedly shared?"[130]

125 Answer provided by a researcher at the Alexander von Humboldt Institute for Internet and Society to CRIN and ddm's questionnaire.

126 CRIN and ddm interview with the Alana Institute, 22 September 2022.

127 Answer provided by Bits of Freedom to CRIN and ddm's questionnaire.

128 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, para. 67, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en

129 CRIN and ddm interview with EDRi, 9 August 2022.

130 CRIN and ddm interview with ECPAT, 23 August 2022.

> *"I don't know who's seen my images, I don't know who will ever see them. I don't want anybody to see them."*[131]

An interviewee with lived experience of online child sexual exploitation and abuse emphasised that "in order to protect children's privacy, we need to be able to identify and remove images [of online abuse]", adding that they would want all those involved, from technology companies to law enforcement, to be doing "every single thing they possibly could to get those images down before anybody saw them."[132]

Across the full spectrum of interviewees who took part in this research, the focus and emphasis of the privacy issues that they addressed varied significantly, but there was a shared recognition that children's privacy matters and is a legitimate concern in regulating encryption.

Understanding children's perspective on privacy[133]

Researchers working with children have warned that "it is vital not to confuse interpersonal with institutional and commercial contexts for privacy, for these contexts differ hugely in who or what one might seek privacy from." They have pointed out that in the common discourse around privacy and children, for example when children are seen to lack a sense of privacy because they share personal information freely with others, or when parents are concerned about grooming, "the focus is children's interpersonal privacy and its safety implications". Children then tend to "(over)extend what they know of interpersonal relations to the operation of platforms. For example, they might talk trustingly of Instagram because so-and-so's father works in technology, and he would surely play fair. They assume ethical reciprocity: if they would never track someone without their knowledge or keep images against someone's will, why would a company?" Children also seem to assume that the way in which they keep their information private from other people (pseudonyms, ghost mode, incognito search, clearing one's history) also keeps it private from companies.

When 11- to 16-year-olds in the UK were encouraged in workshops to think beyond e-safety to how data is processed by schools, doctors, search engines and social media platforms, their attitude changed. "Their confident expressions of agency and expertise would falter, and they would say, outraged: it's creepy, platforms shouldn't be poking around in the online contacts, I want to control who they share my data with and, most tellingly, it's none of their business!"

131 CRIN and ddm interview with the Marie Collins Foundation, 22 November 2022.

132 Ibid.

133 This text is based on findings and quotes from: Prof Sonia Livingstone OBE, *"It's None of Their Business!" Children's Understanding of Privacy in the Platform Society*, 2020, https://freedomreport.5rightsfoundation.com/its-none-of-their-business-childrens-understanding-of-privacy-in-the-platform-society

Encryption and the voices of survivors of child sexual abuse

"It's very easy for people to make assumptions about what we would like or we would say. "[134]

In a 2021 global survey about sexual violence, 54 per cent of respondents said that they had experienced online sexual harms as children.[135] But survivors are not a uniform group; they are diverse, have varied experiences and varied views about all issues, including encryption and online child sexual abuse.

In engaging with survivors throughout this research, some felt that there is already a significant emphasis on privacy - though not necessarily the privacy of victims and survivors - but that not enough attention is being paid to online safety. There was a recognition that there is a consensus about the horrific nature of online child sexual abuse and exploitation and a desire to address it and that victims and survivors' rights must be upheld in achieving this. However, a concern that emerged during interviews was that the severity and urgency of online abuse can be downplayed in how the issue is discussed. As one interviewee explained: "A lot of people do not fully understand the nature of what we're dealing with here, the sophistication of the offenders [...] And most of them have never had to deal with victims or survivors."[136]

Several participants identified conspicuous examples of victim-blaming, particularly in public-facing discussions. For instance, one interviewee expressed their dismay at how a radio magazine programme presented the issue as "perpetrators grooming children online and coercing them into sexually abusing themselves".[137] "Now just think of that language, just think of it. You're talking about children's rights. Their right to be safeguarded is key. And it is actually our duty as adults to safeguard children. Children do not go around sexually abusing themselves. So where do we start with children's rights? We need to start with language."[138]

Many interviewees argued that victims and survivors' voices should be heard more in the debate. They emphasised that even though there are sizeable organisations that argue for the benefit of those who are or have been abused, very rarely are they actually led by people with lived experience. "We need to find a way to include the voices of victims and survivors. Pure, not diluted or interpreted. [...] I've seen far too many professionals going around calling themselves 'survivor consultants' or 'safeguarding consultants with expertise in working with victims and survivors' being consulted by [tech companies] [...] That's second-hand, it's that person's view on it, through their filtering, with their bias. It is not the true, pure voice of the victim and survivor."[139]

One survivor explained, "My voice has been heard in this debate, because I've chosen to speak out. But I don't hear, I don't see very many other people with lived experience having the opportunity to do that at all [...] There has been some engagement [with tech companies], but it was initiated by me. It's still, if I can say, fairly defensive on the tech side. It's not collaborative in any way with victims and survivors, which is quite disappointing because it's such a big issue for us."[140]

This consensus on the need for meaningful inclusion of survivors in reform processes was clear and unambiguous, but it was not a simple expression of support for any specific outcome. Some survivors of child sexual abuse emphasise the need for stronger technological development to address online child sexual abuse material. As one interviewee explained, "For me, the ultimate goal would be for content to be pre-screened prior to upload or sharing. And then it isn't on the platform, it doesn't see the light of day."[141] Other people with lived experience, by contrast, are staunch privacy advocates who are finding it offensive that abuse survivors are being used, as they see it, to "further a political surveillance agenda". They worry that current proposals to protect children online leave the door open for abuse of power and that they would push harmful activities underground, making them more difficult to detect.[142]

The role, possibilities and limitations of technology

"This is a technology and society debate that we haven't really been having so far [...] Technology's kind of happened, the internet's kind of happened [...] and you get to a crisis point where we don't know how to have that debate, and that's where the polarisation comes."[143]

"It is a myth that if you just make the law, then the technologists will figure it out."[144]

The role and potential for technology in tackling online child sexual abuse cuts across the debate on how to regulate the digital space in a way that respects

134 CRIN and ddm interview with the Marie Collins Foundation, 22 November 2022.

135 WeProtect Global Alliance, *Global Threat Assessment 2021*, p. 6, https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021.pdf

136 CRIN and ddm interview with WeProtect Global Alliance, 19 August 2022.

137 The programme was Woman's Hour on BBC Radio 4, 18 November 2022, https://www.bbc.co.uk/sounds/play/m001f5fg

138 CRIN and ddm interview with the Marie Collins Foundation, 22 November 2022.

139 Ibid.

140 Ibid.

141 Ibid.

142 Alexander Hanff, *Why I don't support privacy invasive measures to tackle child abuse*, 11 November 2020, https://www.linkedin.com/pulse/why-i-dont-support-privacy-invasive-measures-tackle-child-hanff

143 CRIN and ddm interview with ECPAT, 23 August 2022.

144 CRIN and ddm interview with Privacy International, 26 September 2022.

human rights, and held a prominent place in the interviews conducted as part of the research for this report.

There was consensus across the spectrum of interviewees of the central role of technology in addressing this issue. Interviewees approaching the issue from a child protection perspective recognised that child sexual abuse is a complex problem with many causes, but stressed that technology plays a key role in the problem. Technology is directly facilitating abuse, enabling the spread of child sexual abuse material on a vastly higher scale than has been possible before. More indirectly, it can also contribute to a culture of normalisation of abuse and the sexualisation of children. Building on this perspective, these interviewees argued that the strong technological aspect must be addressed and technical solutions developed.[145]

Several interviewees thought the focus on technology flows naturally, at least in part, as a consequence of privacy advocates' efforts to find the least intrusive option in terms of interfering with the right to privacy. Suggesting a way forward, one interviewee analysed the problem in this way: "I can't think of anything more necessary than protecting a child from sexual exploitation and abuse. So let's have this debate. Let's look for those technologies that can make legitimate inroads into privacy, but don't impair the essence of this right."[146]

When looking for these solutions, some suggested that companies, particularly those that are very large and politically influential, could research new technologies, consult with governments about what these technologies would look like in practice, and perhaps even get to a point where they can test some of the empirical claims being made.[147]

There was also a note of caution, however, from some organisations working on the issue from a children's rights perspective that technology cannot be a silver bullet, but that given the rhythm of change in the digital world, some technological solutions are needed: "We need to ensure that we have the tools at our disposal that are as good and as modern as the environment that children are inserted into".[148]

The caution about overstating the potential role of technology found its strongest expression among those who warned against "techno-solutionism". They warned of the limitations of the ability of technology to address such a complex problem as online child sexual abuse while upholding fundamental rights.

A significant concern that emerged from interviews was that a focus on technology - and specific technologies in the context of encryption - as the solution risked obscuring the nature of the wider issue.[149] One interviewee framed encryption as a tertiary part of the discussion. They identified the primary level as being about a detailed and comprehensive understanding of the problem of sexual abuse of children online and defining the outcomes that should be achieved in addressing abuse. At a secondary level, they saw a variety of solutions, some of a technological nature and some that were not, that could address aspects of the problem. They considered that encryption, particularly end-to-end encryption, comes into play at a third level of balancing the possible solutions and deciding on those that are most effective. Another interviewee similarly argued, "We need to reframe the debate: what are we actually trying to achieve? Different policy options can be used to try to achieve different outcomes [...] Identifying images is only a means to an end. A higher number of images is not really a key metric in determining success or failure."[150]

A connected theme that emerged was a challenge to the idea that technology can be a quick fix. There were concerns that this idea can lead to broad claims, without the necessary supporting evidence, regarding what various technical proposals can achieve in terms of accuracy and security, and the extent to which they are rights-compliant. One participant stated, "There is an overfocus on encryption in the sense of 'we can't do much against abuse because of encryption' […] and an overbelief in what technology is even able to achieve."[151] Another concluded, "It's a myth that if you just make the law, then the technologists will figure it out."[152]

This expression of the limits of what technology is capable of achieving to address online child sexual abuse and exploitation was most clearly stated in examining particular technological proposals:

> *"The technology on prevention doesn't exist yet. When you look at things like grooming, for example, the notion of trying to predict what language somebody might use… if we can't do that in real life, which we can't - we can't unfortunately predict what language somebody with that intent would use - then technology can't do that either because the data and input obviously has to come from the real world. So I would definitely say that on prevention, it is particularly dubious to turn to technology for a solution."*[153]

Among those interviewees who were critical or cautious about the possibilities of technology to address online child sexual abuse and exploitation, substantial debate emerged about the role that specific technologies could play and who can have a legitimate role in employing these technologies.

145 These points were made mainly in CRIN and ddm's interview with WeProtect Global Alliance, 19 August 2022.
146 CRIN and ddm interview with a civil society representative, 12 August 2022.
147 Some of these points were made in CRIN and ddm's interview with Ian Brown, 6 October 2022.
148 CRIN and ddm interview with the Alana Institute, 22 September 2022.
149 CRIN and ddm conversation with a civil society representative, 1 June 2022.
150 CRIN and ddm interview with 5Rights, 5 September 2022.
151 CRIN and ddm interview with EDRi, 9 August 2022.
152 CRIN and ddm interview with Privacy International, 26 September 2022.
153 CRIN and ddm interview with the Centre for Democracy and Technology (Europe Office), 13 October 2022.

The role of law enforcement

One interviewee who approached this issue from the perspective of the right to privacy, explored the potential for the use of existing technology and existing powers that would not require further legislation or regulation in many jurisdictions:

> *"[T]here are many technologically-based investigative techniques right now that law enforcement have access to that do not require the breaking of encryption. So, for instance, if they have a particular suspect, they can get a warrant to seize their device and then look at what's on the device itself. Or they can get a warrant to look at the metadata of particular communications."*[154]

This approach that relies on the use of law enforcement powers by law enforcement authorities was a common theme across several interviews. A challenge that was posed in the context of online child sexual abuse and exploitation, however, was addressing the scale the abuse. Looking at the ubiquity of the Internet and the proliferation of illegal material, some interviewees explained that "you realise that you can't moderate your way out of that with just people checking", and that some intensive intervention in the form of automation is necessary.[155]

For some, this challenge is unavoidable if the matter is treated as within the remit of law enforcement. Others questioned this framing, in particular arguing that the narrative of "stranger danger" is not supported by evidence.[156] They further argued that if child sexual abuse is more often than not perpetrated not by strangers, but by family members and others known to the child, for example teachers and religious figures, then proposals for protecting children might need to focus more on the role of law enforcement in identifying these perpetrators, and less on the use of automation to detect child sexual abuse material in all private communications. Others, sometimes acknowledging the dangers of relying too heavily on the "stranger danger" narrative, sounded a note of caution about the capacity of law enforcement to fulfil their role in general.

One interviewee from the UK, who has been working in this space for almost 25 years, said: "The police service has deteriorated in the last 10 years [...] The police were getting a lot better, but unfortunately that has gone back and that, I think, is mainly a result of lack of funding and very experienced officers being laid off because they're more expensive [...] But experience is hugely valuable, it's about mentoring new officers etc."[157] The interviewee also stressed the importance of investing in providing a standard level of training to law enforcement: "Some teams I've dealt with have been absolutely abysmal. Some have been absolutely fantastic. So it's a bit of a lottery."[158]

Training has been flagged as particularly important where police officers need to speak directly to children who are potential victims of abuse. Another UK-based interviewee explained the lack of sensitivity and trauma-informed interviewing techniques, "[T]hey are called to the school because the child has got an image on their phone. How do they have that conversation? They don't know. And it's not because they don't want to know, it's because we're cramming their training in such a short period of time."[159] A participant warned that, if funds are lacking with regard to basic features like officer training, it cannot be expected that the police would be able to apply more innovative investigation methods, for example going undercover in video games and using the in-game microphone and chat in order to speak to children in confidence and identify instances of abuse.[160]

This assessment of a deterioration in law enforcement's capacity to address child sexual abuse and exploitation was also met with a wariness of overly empowering law enforcement entities:

> *"There is an overarching trend across the European region and globally for a creep of power for law enforcement and a dilution of checks and balances on that power."*[161]

This concern was particularly evident in discussions about marginalised children, who are more likely to have negative experiences of policing, including racism. Some participants warned that technology-enabled police surveillance of disadvantaged communities would worsen injustice and would contribute to a climate of impunity.[162] One interviewee perceived a lack of consistency at the European level in discussions about law enforcement and artificial intelligence, on the one hand, and technologies for detection of child sexual abuse, on the other. "I would say there is very strong agreement at the moment [regarding the EU AI Act proposal] that law enforcement deploying AI is high-risk and needs to be heavily regulated. So it's extraordinary that in the [EU CSA Regulation proposal] we then have law enforcement using different degrees of AI with the most vulnerable children".[163]

154 CRIN and ddm interview with Privacy International, 26 September 2022.

155 CRIN and ddm interview with IWF, 3 November 2022.

156 WeProtect Global Alliance, *Global Threat Assessment 2021*, p. 6.

157 CRIN and ddm interview with One in Four, 14 November 2022.

158 Ibid.

159 CRIN and ddm interview with the Marie Collins Foundation, 22 November 2022.

160 One example given was the Undercover Avatar project by the youth protection association L'Enfant Bleu: https://www.cresta-awards.com/?action=ows:entries.details&e=97352&project_year=2022

161 CRIN and ddm interview with the Centre for Democracy and Technology (Europe Office), 13 October 2022.

162 For a discussion of the risks posed by data-driven approaches to policing, see: BBC, *Civil liberties group says data not silver bullet to reduce crime*, 24 November 2022, https://www.bbc.com/news/uk-england-oxfordshire-63730451

163 CRIN and ddm interview with the Centre for Democracy and Technology (Europe Office), 13 October 2022.

The wider ecosystem

The limitations of detection technologies and the practical restrictions on what law enforcement can achieve even with these technologies led a number of interviewees to call for a systems approach to the problem of online child sexual abuse. As one participant explained, "The more we learn about it, the more we realise that it requires lots of different interventions. [...] There is not one magic thing. You should be doing everything."[164]

An opportunity for consensus emerged from interviewees when the value and merits of any particular technological application were put into context.

> *"System design and the design of the services also play a huge part. And, in fact, many of these services could make relatively small adjustments - whether adults can contact children directly, whether they are able to befriend or follow a child - you know, some of these kinds of designs as a way of preventing grooming pathways."*[165]

This recognition that no individual application of technology will prevent and secure redress for online child sexual abuse and exploitation, but that many small adjustments in conjunction can be effective, sets out a space where the potential for consensus could be explored.

Beyond prevention by design and the interconnectedness of the online space, many participants emphasised the need to pay more attention to the various actors in the wider ecosystem. Some suggested that the excessively narrow focus on finding a technological silver bullet is a product of politics: it is more convenient to put forward proposals to tackle abuse without seeming to violate human rights than to recognise that there are still many unanswered questions and that long-term effective solutions to what is ultimately a societal problem are difficult to achieve.

Therefore a number of interviewees called for some honest conversations about the need for state as well as business investment at various levels. They identified schools and the health sector as vital actors, and suggested that there should be an increased focus on: digital literacy, particularly among young people to make them better understand the risks of generating material of themselves and sharing it with people they know; awareness raising among parents about how technology might be used by their children, as well as better equipping doctors and other health professionals to identify the physical and psychological signs of abuse.

> *"Social workers, teachers, we're all letting victims and survivors down. And that's not because we don't have the will [to fight against abuse], it's because we don't have the resources to."*[166]

164 CRIN and ddm interview with IWF, 3 November 2022.
165 CRIN and ddm interview with 5Rights, 5 September 2022.
166 CRIN and ddm interview with the Marie Collins Foundation, 22 November 2022.

> *"I didn't get therapy for nine years after my experience [of abuse]. That's never ok. There need to be resources put into recovery as well."*[167]

Social services in particular were the focus of some animated discussions in interviews. A clear need for investment was identified by many. As one interviewee who worked as a social worker in the UK public sector before transitioning to the charity sector explained, "I couldn't make a difference in our political climate. Experienced social workers were leaving left, right and centre. Good ones move on. [...] Whenever you have austerity, the first thing that goes is training. The second is staff morale."[168] A particularly important area which deserves considerably more attention, as pointed out by an interviewee with lived experience, are recovery services.[169]

All these investments, it was said in some interviews, should be complemented by deeper research into what drives the behaviour of abusers, starting, for example, with a real questioning of the phenomenon of sexualisation of children, which - as some survivors have emphasised - has been hugely profitable for the advertising, fashion and entertainment industries.[170] Some also suggested that there should be interventions into known offenders while they are incarcerated or on probation, and a much stronger focus on rehabilitation in the criminal justice system.

Beyond self-regulation

The role of online platforms - particularly, but not exclusively, large technology companies - has been part of the debate about online regulation for decades. Diverse views emerged from the interviewees that took part in the research for this report about the best way of achieving effective online regulation, but from first principles there was a great deal of consensus.

There was broad agreement that under international human rights standards, States have a duty to respect, protect and fulfil children's rights, which applies in the context of business activities.

There was also a general consensus that the impact that platforms have on society is so significant that the era of self-regulation is over. As one interviewee argued, "There does need to be a degree of oversight, and democratic oversight is preferable in many cases."[171]

167 Ibid.
168 Ibid.
169 Ibid.
170 Alexander Hanff, *Why I don't support privacy invasive measures to tackle child abuse*, 11 November 2020.
171 CRIN and ddm interview with Richard Wingfield, 6 September 2022.

There was also agreement that there is a lack of uniformity or transparency regarding the way that platforms tackle child sexual abuse material in the absence of regulation. Interviewees saw a discrepancy that should be addressed and identified the need for clear guidance to the companies to tell them what is expected of them and how they are supposed to do it. There were strong arguments in favour of consistency and accountability. Advocates whose work focused specifically on the internet saw the values of openness and trust as essential for the Internet to flourish and that technology must be trustworthy and secure for this to be achieved.[172]

Beyond this broad basis of agreement, divergence began to enter the frame around the precise role and functioning of regulation, including where to place the burden for action. A common trend that emerged from most privacy and technology-focused actors was that if too great an emphasis is placed on the responsibilities of businesses to detect criminal activity, particularly related to child sexual abuse, there was a risk of privatising law enforcement functions. They were concerned about the shirking of responsibility on the part of democratically-elected governments and the passing of the buck to politically unaccountable platforms. They warned that this would lead to a dependence on monopolistic tools built by private actors, to the detriment of traditional methods of investigation and prosecution.[173]

A similar concern that emerged from interviews was that where platforms are overly empowered, this can have an impact on disempowering other services, such as social services and education actors. An overfocus on platforms would lead to a narrow concern with technological solutions and a corresponding failure to fully take into account the roles that other services play, their needs and how they interact in the wider ecosystem.

By contrast, interviewees who emphasised the focus on technology as natural tended to highlight that, ultimately, the tools that private companies build benefit law enforcement, as they are being used to report child sexual exploitation and abuse to authorities.[174]

Beyond Europe and North America

For laws to be effective, they must be well tailored to national contexts and regulatory structures. The same law transplanted from one jurisdiction to another can also have significantly different impact and implementation. As one interviewee expressed the challenge: "[t]here is the danger of replicating legislation from one jurisdiction in another. It's always important to have these widespread, public, transparent consultations, in order to develop legislation that's tailored to each jurisdiction."[175]

One participant highlighted that those working outside Europe and North America face a particular set of challenges in dealing with the issue of platform regulation.[176] Since the Big Tech are mostly based in the US and Europe, most of their approaches and resources are directed towards these geographical areas.[177] Research has highlighted the phenomenon of "design discrimination", whereby some children are afforded less privacy and less protection on a platform than other children on the same platform, depending on where in the world they live.[178] Consequently, there needs to be substantially more engagement between platforms and countries outside Europe and North America, which form a high proportion of the user base, in order to take diverse contexts and specificities into account. For example, the technological solutions that platforms might adopt in order to protect children's rights online need to be compatible with the wide variety of devices that children use across the world. Crucially, this includes low-end devices. Another concern is around children's access to the Internet. An important example here is the practice of zero-rating particularly in developing markets: offering packages that provide cost-free access to particular applications and services. The platforms that children have free access to will in practice control the flow of information. Whether these platforms are encrypted or not will have a disproportionate impact on children if they are not able to access alternatives.

The interviewee argued that there is a particular tension at play. On the one hand, countries outside the Anglo- and Euro-centric spaces need to make more efforts to put in place regulation to hold platforms to account. Otherwise, there is a real danger that, in jurisdictions where regulation is less advanced, platforms will not extend the same protections that they are extending to children from countries "closer to the decision centre". At the same time, regulation is a difficult and slow process, so realistically, in some jurisdictions it will constantly lag behind platforms' initiatives. In this case, platforms must still be pressured to take proactive steps in protecting children's rights in the digital environment. This could be achieved, for example, by making creative use of legislation that is not specifically about encryption, like child protection or consumer protection laws.

172 These points were most clearly made in CRIN and ddm's interview with ISOC, 30 August 2022.

173 CRIN and ddm conversation with a civil society representative, 1 June 2022.

174 WeProtect Global Alliance and ECPAT International, *Technology, privacy and rights: keeping children safe from child sexual exploitation and abuse online - Expert Roundtable Outcomes Briefing*, 8 April 2021, https://www.weprotect.org/wp-content/uploads/Technology-privacy-and-rights-roundtable-outcomes-briefing.pdf

175 CRIN and ddm interview with a civil society representative, 12 August 2022.

176 These points were made in CRIN and ddm's interview with the Alana Institute, 22 September 2022.

177 One example given was Facebook's language gap in content moderation: WIRED, *Facebook Is Everywhere; Its Moderation Is Nowhere Close*, 25 October 2021, https://www.wired.com/story/facebooks-global-reach-exceeds-linguistic-grasp/

178 Fairplay, *Global platforms, partial protections: Design discriminations on social media platforms*, July 2022, https://fairplayforkids.org/wp-content/uploads/2022/07/design-discriminations.pdf

The impact of encryption on children's rights

This chapter explains the human rights framework that applies to children's rights, and analyses the implications of encryption for these rights, with a particular focus on children from disadvantaged or marginalised communities.

The international human rights framework

Human rights - for children as for adults - are interdependent, non-hierarchical and mutually reinforcing. To give effect to them, they must be read and applied together and in their entirety.

All States, with the exception of the US, have ratified the Convention on the Rights of the Child ("CRC").[179] It is the world's most ratified human rights treaty and so provides an internationally agreed basis for the scope and content of children's rights. The CRC recognises civil and political rights as well as economic, social and cultural rights. The practice and jurisprudence of the Committee on the Rights of the Child ("the Committee"), through its General Comments, Communications and State Reviews, also provides authoritative guidance on how the CRC applies.

General principles

Within the CRC, the four "general principles" stand as rights in themselves and as tools to interpret and apply the other rights within the Convention.

Non-discrimination (Art. 2 CRC)

States must ensure that all of the rights within the CRC are respected for all children, without discrimination. The grounds of prohibited discrimination set out in the CRC are non-exhaustive and, to date, the Committee has recognised more than 50 grounds of prohibited discrimination. As the Committee has explained, this right requires children to have equal and effective access to the digital environment and that they not be discriminated against by being excluded from using digital technologies and services, or by receiving hateful communications or unfair treatment through those technologies.[180]

179 Convention on the Rights of the Child, available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

180 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, paras. 9-11.

Best interests of the child (Art. 3 CRC)

In all actions concerning children, their best interests must be a primary consideration. This right has three aspects:[181]

1. A substantive right: when making decisions that affect children States must reach an outcome that treats the best interests of children as a primary consideration.
2. A procedural right: wherever a decision is made that will affect a child, a group of children or children in general, the process must include an evaluation of the impact of the decision on the children.
3. An interpretive right: if a legal provision is open to more than one interpretation, the interpretation which most effectively serves the best interests of the child must be chosen.

Any consideration of what is in the best interests of the child must include respect for children's right to be heard and children's views must be given due weight.

Right to life, survival and development (Art. 6 CRC)

All children have the right to life and States are required to ensure to the maximum extent possible the survival and development of the child. Regarding the digital environment, the Committee has specifically highlighted risks "relating to content, contact, conduct and contract encompass, among other things, violent and sexual content, cyberaggression and harassment, gambling, exploitation and abuse, including sexual exploitation and abuse, and the promotion of or incitement to suicide or life-threatening activities, including by criminals or armed groups designated as terrorist or violent extremist."[182]

Right to be heard (Art. 12 CRC)

Children have the right to express their views freely in all matters that concern them and for those views to be given due weight in accordance with their age and maturity. This is not only a procedural right requiring them to have the opportunity to give their views, but also requires States to act on those views. The right also applies not only to decisions that affect an individual child, but also to those that affect children as a group.[183] The Committee has recommended that States "should involve all children, listen to their needs and give due weight to their views. They should ensure that digital service providers actively engage with children, applying appropriate safeguards, and give their views due consideration when developing products and services."[184]

Other key rights in the context of encryption

Evolving capacities (Art. 5 CRC)

Even though it is not in itself a general principle of the CRC, the concept of "evolving capacities" plays an important role in the realisation and application of children's rights. It refers to the responsibility of parents (and others) to "continually adjust the levels of support and guidance they offer to a child", depending on the "child's interests and wishes", as well their "capacities for autonomous decision-making" and understanding of their best interests.[185]

Violence against children (Arts. 19, 34, 39 CRC)

States are required to take all appropriate legislative, administrative, social and educational measures to protect children from all forms of violence, including physical, mental and sexual violence. These protective measures should include social programmes to provide support to children and those who care for children, as well as other measures for prevention, identification, reporting, referral, investigation, treatment and follow-up to instances of maltreatment. States are also required to take all appropriate measures to promote the physical and psychological recovery of child victims of violence.

Freedom of expression (Art. 13 CRC)

Children have the right to free expression, including the freedom to seek, receive and impart information and ideas of all kinds. This right may be subject to restrictions where provided by law and necessary for the respect of the rights or reputations of others and for the protection of national security, public order, or of public health or morals. Applying this right, the Committee has stated that "[a]ny restrictions on children's right to freedom of expression in the digital environment, such as filters, including safety measures, should be lawful, necessary and proportionate. The rationale for such restrictions should be transparent and communicated to children in age-appropriate measures." [186] The Committee has also recommended that States should protect children from cyber aggression and threats, censorship, data breaches and digital surveillance.[187]

181 See, UN Committee on the Rights of the Child, *General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration*, CRC/C/GC/14, 29 May 2013, para. 6, available at: https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf

182 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, para. 14.

183 See, for example, UN Committee on the Rights of the Child, *General comment No. 12 (2009) - The right of the child to be heard*, CRC/C/GC/12, https://www2.ohchr.org/english/bodies/crc/docs/advanceversions/crc-c-gc-12.pdf

184 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, para. 17.

185 See, for example, UN Committee on the Rights of the Child, *General comment No. 7 (2005) - Implementing child rights in early childhood*, CRC/C/GC/7/Rev.1, 20 September 2006, para. 17, https://www2.ohchr.org/english/bodies/crc/docs/AdvanceVersions/GeneralComment7Rev1.pdf

186 UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, para. 59.

187 Ibid.

Access to information (Arts. 13, 17 CRC)

In addition to the recognition of children's right to seek and receive information and ideas of all kinds, the CRC requires States to ensure that children have access to information and material from a diversity of national and international sources, especially those aimed at the promotion of social, spiritual and moral well-being and physical and mental health. The Committee has recommended that States ensure that digital service providers comply with relevant guidelines, standards and codes and enforce lawful, necessary and proportionate content moderation rules, but that content moderation and controls are balanced with the right to protection of children's other rights, including their rights to freedom of expression and privacy.[188]

Freedom of association and peaceful assembly (Art. 15 CRC)

Children have the right to freedom of association and peaceful assembly. This right must not be restricted except in conformity with the law and necessary in a democratic society in the interests of national security or public safety, public order, the protection of the public health or morals or the protection of the rights and freedoms of others. The Committee has recognised that "[p]ublic visibility and networking opportunities in the digital environment can also support child-led activism and can empower children as advocates for human rights", and "that the digital environment enables children, including children human rights defenders, as well as children in vulnerable situations, to communicate with each other, advocate for their rights and form associations."[189]

Right to privacy (Art. 16 CRC)

No child shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, nor to unlawful attacks on their honour and reputation. Children are entitled to the protection of the law against such interference or attacks. The Committee has recognised that privacy is vital to children's agency, dignity and safety and for the exercise of their rights.[190]

Right to the highest attainable standard of health (Art. 24 CRC)

Children have a right to the highest attainable standard of health. In the context of the digital environment, the Committee has recognised the desire from children for "access to free, confidential, age-appropriate and non-discriminatory mental health and sexual and reproductive health services online" and recommended that States "ensure that children have safe, secure and confidential access to trustworthy health information and services, including psychological counselling services." The Committee has also recommended that "[t]hose services should limit the processing of children's data to that which is necessary for the performance of the service and should be provided by professionals or those with appropriate training, with regulated oversight mechanisms in place."[191]

Access to justice

The Committee has recognised that children face particular challenges in enforcing their rights related to the digital environment, for example because of the lack of specific legislation, the difficulties in identifying perpetrators, or the lack of knowledge of their rights. The Committee therefore stated that States should ensure that appropriate and effective remedies are available for violations of children's rights, including in the digital environment. States should provide for complaint and reporting mechanisms that are free, safe, confidential, responsive, child-friendly and accessible. They should also establish frameworks for the referral of cases and provide effective support to children who are victims. In particular, they should provide specialised training for law enforcement officials, prosecutors and judges. States should also ensure that businesses provide effective complaint mechanisms, and that agencies with oversight powers relevant to children's rights investigate complaints and provide adequate remedies for violations of children's rights.[192]

The table below sets out an analysis of how the full range of children's rights are engaged by encryption, whether positively or negatively.

188 Id., para. 56.
189 Id., para. 66.
190 Id., para. 67.
191 Id., para. 94
192 Id., paras. 43-49

The right	The benefits of encryption	The risks of encryption
Non-discrimination (Art. 2 CRC)	• Encryption protects the communication of all children, including those who are not aware of the benefits of encryption. • It poses specific benefits to children from disadvantaged or marginalised groups, who face more risks online based on what they communicate, e.g. LGBT+ children, Indigenous children, children from ethnic or religious minorities, children affected by domestic violence, children engaged in political activism in settings where that poses a risk, children with disabilities. • Encryption protects women and girls against the involuntary disclosure of information, where they face particular threats of surveillance, harassment and violence online.	• Content that promotes discrimination, either generally or against specific children, can be circulated undetected in encrypted platforms. • If law enforcement does not have access to communications because they are encrypted, they might use other data (such as metadata or behavioural signals) in a discriminatory manner.
Right to life (Art. 6 CRC)	• Encrypted platforms keep communications private, which ensures the safety of those who would otherwise be targeted in a way that puts their lives at risk, based on the content of their communications.	• Encrypted platforms facilitate the sharing, undetected, of communications that endanger the lives of children (e.g. incitement to suicide, hate speech and incitement to violence that could result in deaths, the planning of terrorist attacks or other crimes). • Children who have been subjected to sexual abuse perpetrated by means of encrypted channels might try to self-harm or take their lives.
Right to be heard. Freedom of expression and information (Arts. 12, 13 CRC)	• The privacy afforded by encryption bolsters children's freedom of expression and information. It provides them with the opportunity to express their opinions and seek, receive and impart information on a variety of topics, including political, social, cultural and religious issues, without fear of repercussions. This is particularly true of children from disadvantaged or marginalised groups.	• The spread of "bad-information" like disinformation or hate speech through encrypted channels can lead children to censor themselves when seeking information. • Children cannot access encrypted information of interest to them or the general public without the key.
Freedom of thought, conscience and religion (Art. 14 CRC)	• Religious minorities can use encrypted channels to communicate securely. • By protecting the privacy of their communications, encryption can uphold the freedom of thought of those whose beliefs might not be widely accepted in society (e.g. abortion rights advocates). • Platforms themselves cannot monitor the content of end-to-end encrypted communications, therefore they do not have data that allows them to "manipulate or interfere with children's right to freedom of thought and belief in the digital environment, for example by emotional analytics or inference".[193]	• Encrypted channels can be used to propagate hate speech against religious minorities, or circulate information that threatens children's freedom of thought.[194]

193 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, para. 62.

194 The impact of technology on freedom of thought is an underexplored issue, particularly regarding the manipulation of users' emotions. In 2017, it was reported that Facebook showed advertisers how it can identify emotional data of its young users: The Guardian, *Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'*, 1 May 2017, https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens. Previously the company had published the results of an experiment in which it manipulated information posted on 689,003 users' news feed and found that peoples' emotions were reinforced by what they saw, in an "emotional contagion" process: The Guardian, *Facebook emotion study breached ethical guidelines, researchers say*, 30 June 2014, https://www.theguardian.com/technology/2014/jun/30/facebook-emotion-study-breached-ethical-guidelines-researchers-say

Freedom of association and freedom of peaceful assembly (Art. 15 CRC)	• Encryption can enable child protesters to organise without fear of being targeted for reprisals.	• Encrypted platforms could be used to propagate hate speech about certain children or groups of children (especially those disadvantaged or marginalised), who could become fearful of exercising their freedoms of association and assembly.
Privacy (Art. 16 CRC)	• By limiting the number of people who can see what information children exchange online or access their data, encryption benefits children's privacy. Knowing that they are not being continuously surveilled, whether online or offline, helps children to build trust with parents, teachers or others they have personal relationships with, and makes it more likely that they will ask for help when they need it. • Privacy and trust-building are particularly important for children who have a higher risk of being targeted for what they communicate about, especially those from disadvantaged or marginalised communities.	• Encrypted services might be used to disseminate content that violates children's privacy, such as non-consensual information and child sexual abuse material.
Protection from information and material injurious to well-being (Art. 17(e) CRC)	• There is a danger that the protection language in Art. 17 CRC is misused to justify bans on certain types of information being made available to children (e.g. the 'gay propaganda' ban in Russia and some countries in Eastern Europe and Central Asia) or that it is misapplied to promote prejudice among children (e.g. through racist propaganda). Where this is the case, those who organise against the misuse of protection language can use encrypted channels to avoid being targeted.	• Encrypted channels can be used to disseminate information injurious to children's well-being, such as child sexual abuse material or hate speech. They make it difficult to identify and remove such content and identify perpetrators.

Protection from violence and exploitation (Art. 19 CRC)	• Encrypted services can protect children from being targeted for violence based on information they send or receive, especially where they are part of disadvantaged or marginalised groups. • Access to children's personal data can make them vulnerable to grooming and exploitation, but encryption helps to keep the data secure. • Children who are sexually exploited can communicate securely through encrypted channels in order to ask for help, store or send evidence, etc.	• Encryption can facilitate violence against children, in particular sexual abuse, for example by allowing perpetrators to access and disseminate child sexual abuse material online undetected. • Encryption keeps the communications between the child and the perpetrator private in the case of grooming, bullying or harassment, making it more difficult to investigate and prosecute abuse.
Health and health services (Art. 24 CRC)	• Patients' data can be shared and stored securely thanks to encryption. • Encrypted platforms facilitate the sharing of information about health, especially where it might otherwise be censored (e.g. parents sharing pictures of their children's health condition where automated tools might block them; information about HIV prevention and treatment shared by LGBT+ groups).	• Disinformation about health can circulate in encrypted channels without being detected. • Encrypted platforms can be used to disseminate information that threatens children's health, for example on eating disorders or self-harm. • Encrypted platforms can be used to facilitate violence against children, putting at risk their physical and mental health.
Adequate standard of living (Art. 27 CRC)	• Encryption facilitates secure financial transactions.	
Right to education (Art. 28 CRC)	• Encrypted channels can be used to share educational and vocational information and guidance which would otherwise be censored.	

Right to leisure, play and culture (Art. 31 CRC)	• Encrypted platforms can be used to share information that facilitates children's participation in cultural, artistic, recreational and leisure activity in contexts where this information might otherwise be censured.	
Sexual exploitation (Art. 34 CRC)	• Access to children's personal data can make them vulnerable to grooming and exploitation, but encryption helps to keep the data secure. • Children who are sexually exploited can communicate securely through encrypted channels in order to ask for help, store or send evidence, etc.	• Encryption can facilitate child sexual exploitation and abuse, for example by allowing perpetrators to communicate with each other, or to access and disseminate child sexual abuse material online undetected. • Encryption keeps the communications between the child and the perpetrator private in the case of grooming, making it more difficult to investigate and prosecute abuse.
Abduction, sale and trafficking (Art. 35 CRC)	• Trafficked children can communicate securely through encrypted channels in order to ask for help, store or send evidence.	• Encrypted platforms can be used by child traffickers to facilitate the abduction, sale and trafficking of children.
Protection of children affected by armed conflict (Art. 38 CRC)	• During armed conflicts, encrypted messaging ensures secure communication among civilians, including children.	• During armed conflict, encrypted channels can be used to plan activities which threaten the right to protection of civilians, including children.
Child justice (Art. 40 CRC)	• Encrypted data storage and transfer, for example regarding court cases involving children, can facilitate the smooth and secure administration of child justice. • By using encryption, law enforcement can prevent leaks of investigative material.	

Privacy: its scope, the link with protection, and permissible restrictions

The right to privacy - for children and for adults - has formed a central part in the debate about the regulation of encryption. A more detailed analysis of the right to privacy, however, and its permissible restrictions can set out a framework for how to engage with regulation of encryption in a way that is children's rights respecting, including where there may be tensions in the application of children's rights more broadly.

Scope

Children's right to privacy is well established in international human rights law. It is enshrined in a number of treaties and declarations,[195] including, as seen above, in the CRC, which prohibits the arbitrary or unlawful interference with children's privacy or correspondence.[196] The protection of the right to privacy under the CRC is identical to that under the International Covenant on Civil and Political Rights, with the exception of the introduction of the word "child", indicating an equivalent protection for the privacy of children as for adults.

The right to privacy plays an important role in children's development. The Committee has stated that "[p]rivacy is vital to children's agency [and] dignity".[197] The right to respect for private and family life under the European Convention on Human Rights, for example, has been interpreted as protecting "the right to personal development, whether in terms of personality or of personal autonomy".[198] It also includes "the right for each individual to approach others in order to establish and develop relationships with them and with the outside world, that is, the right to a 'private social life'".[199]

Privacy and protection

As the Committee has recognised, privacy enables the "exercise of [children's] rights". Sometimes referred to as an "enabling" or "gatekeeper" right,[200] privacy

195 For example, Art. 17 of the International Covenant on Civil and Political Rights, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights; Art. 12 of the Universal Declaration of Human Rights, https://www.un.org/en/about-us/universal-declaration-of-human-rights

196 Art. 16 of the Convention on the Rights of the Child.

197 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, para. 67.

198 *Bărbulescu v. Romania* [European Court of Human Rights, Grand Chamber], App. No. 61496/08, 5 September 2017, para. 70.

199 Id., paras. 70-71. See also: European Court of Human Rights (Registry), *Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence*, updated on 31 August 2022.

200 Lorna McGregor, *First Report of the UN Special Rapporteur on the Right to Privacy to the Human Rights Council*, EJIL: Talk!, 18 March 2016, https://www.ejiltalk.org/first-report-of-the-un-special-rapporteur-on-the-right-to-privacy-to-the-human-rights-council/

facilitates the enjoyment of other rights including freedom of expression and information, freedom of association, freedom of thought, conscience and religion, right to health and non-discrimination.

The Committee has also acknowledged that privacy is vital to children's dignity, safety and the exercise of their rights.[201] Therefore the Committee recognised that privacy is not opposed to the protection of children from violence - instead, privacy has a protection element to it. Indeed, violations of the right to privacy can have very serious consequences, including physical or psychological harm. This is particularly true for children from disadvantaged and marginalised groups, as discussed below.

Restrictions

The right to privacy is qualified, not absolute, so it may be restricted in certain circumstances.

As the Committee has explained, this means that any interference with children's privacy should be "provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimisation, be proportionate and designed to observe the best interests of the child and must not conflict with the provisions, aims or objectives of the Convention".[202] According to the UN Human Rights Committee, restrictions on privacy cannot "impair the essence" of the right.[203]

Regarding encryption specifically, the Committee on the Rights of the Child has stated that, "[w]here encryption is considered an appropriate means, States parties should consider appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material".[204] It reaffirmed the boundaries of permissible limitations under international human rights law, adding that the measures "must be strictly limited according to the principles of legality, necessity and proportionality".[205]

The Committee has suggested that routine and indiscriminate measures are not necessary and proportionate. For example, the Committee has highlighted that practices like automated data processing, mandatory identity verification, information filtering and mass surveillance are "becoming *routine* [emphasis added]" and "may lead to arbitrary or unlawful interference with children's privacy", which could continue to affect them later in life.[206] Therefore it has stated that digital surveillance and associated automated data processing should respect children's privacy and "should not be conducted *routinely*, *indiscriminately* [emphasis added] or without the child's knowledge". It also emphasised that "consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose."[207]

The UN High Commissioner for Human Rights has used similar language, warning that a "widespread and indiscriminate impact [on the right to privacy] is not compatible with the principle of proportionality".[208] The Commissioner observed that "most encryption restrictions on [privacy and associated rights] are disproportionate, often affecting not only the targeted individuals but the general population".[209] The Commissioner then cautioned against "all direct, or indirect, general and indiscriminate restrictions" on the use of encryption.[210]

Regional courts have also used comparable language in judgments. Regarding persons suspected, but not convicted of offences, the European Court of Human Rights, for example, held that "the blanket and indiscriminate nature of [retention of fingerprints and DNA]" did not strike "a fair balance between the competing public and private interests", and therefore was not a necessary and proportionate interference with the right to respect for private life.[211] Regarding traffic and location data, the Court of Justice of the European Union held that the only instance when "the general and indiscriminate retention" and "the automated analysis" of this data can be proportionate is when the duration of the retention is strictly necessary to respond to a serious, genuine, present or foreseeable threat to national security.[212] Regarding the content of electronic communications, the Court used even stronger language, indicating that laws which allow public authorities "access on a generalised basis" to content data compromise the essence of the right to respect for private life.[213]

---

201 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, para. 67.

202 Id., para. 69.

203 UN Human Rights Committee, *General Comment No. 31 (2004): The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, 26 May 2004, para. 6, https://www.refworld.org/docid/478b26ae2.html; UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/51/17, 4 August 2022, para. 56.

204 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, para. 70.

205 Ibid.

206 Id., para. 68.

207 Id., para. 75.

208 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29, 3 August 2018, para. 20.

209 UN High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/51/17, 4 August 2022, para. 25.

210 Id., para. 57 (b)

211 *S. and Marper v. the United Kingdom* [European Court of Human Rights], App. Nos. 30562/04 and 30566/04, 4 December 2008, para. 125.

212 *La Quadrature du Net and Others v. Premier ministre and Others* [Court of Justice of the European Union, Grand Chamber], Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020, para. 177.

213 *Maximillan Schrems v. Data Protection Commissioner* [Court of Justice of the European Union, Grand Chamber], Case C-362/14, 6 October 2015, para. 94.

The role of businesses

Private companies play a crucial role in the debate on encryption and children's rights due to their key place in the digital environment. While the Convention sets out the obligations of States with regard to children's rights, the Committee has recognised that duties and responsibilities to respect those rights also extend in practice to businesses.[214]

The Committee has acknowledged the relevance of the UN "Protect, Respect and Remedy" ("PRR") Framework and the Guiding Principles on Business and Human Rights, as well as the Children's Rights and Business Principles.[215] The PRR Framework[216] sets out three principles: (1) the State duty to protect against human rights abuses by third parties, including business; (2) the corporate responsibility to respect human rights; and (3) the need for more effective access to remedies. The UN Guiding Principles on Business and Human Rights[217] are a set of principles to assist States and businesses in implementing the PRR Framework. Regarding businesses, the principles rest on two elements: a policy commitment to respect human rights, and a human rights due diligence process. The Children's Rights and Business Principles[218] set out business actions to respect and support children's rights. The Committee has stated that "all businesses must meet their responsibilities regarding children's rights and States must ensure they do so."[219]

Regarding the digital environment specifically, the Committee has affirmed that "[b]usinesses should respect children's rights and prevent and remedy abuse of their rights in relation to the digital environment", while States "have the obligation to ensure that businesses meet those responsibilities."[220] The Committee has recognised that "[a]lthough businesses may not be directly involved in perpetrating harmful acts, they can cause or contribute to violations of children's right to freedom from violence, including through the design and operation of digital services". It has also stated that "[States] should require [businesses] to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services."[221]

214 UN Committee on the Rights of the Child, *General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*, CRC/C/GC/16, 17 April 2013, para. 8, https://www2.ohchr.org/english/bodies/crc/docs/CRC.C.GC.16.pdf

215 Id., para. 7

216 Available at: https://www2.ohchr.org/english/bodies/hrcouncil/docs/8session/a-hrc-8-5.doc

217 Available at: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

218 Available at: https://www.unicef.org/media/96136/file/Childrens-Rights-Business-Principles-2012.pdf

219 UN Committee on the Rights of the Child, *General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*, CRC/C/GC/16, 17 April 2013, para. 8.

220 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, para. 35.

221 Id., para. 39.

Beyond the "privacy versus protection" paradigm: some scenarios

"There is no single, monolithic vision of what it means to be a child."[222]

The full range of children's rights interact across the debate on encryption, beyond any analysis built exclusively on privacy versus protection. The following scenarios explore various ways in which encryption impacts children's rights, especially where those children belong to disadvantaged or marginalised groups. This section does not aim to provide an exhaustive discussion of the ways in which encryption might be relevant to them. Instead, it seeks to present situations that give a flavour of the breadth and complexity of the ethical, legal and practical issues at stake. These scenarios are intended to open up the discussion beyond the paradigm of encryption as a question of privacy or protection. The aim is to showcase children's agency - their ability to make decisions and exercise their rights in a variety of public and private settings, and in relation to others, such as the State, their family and community, and of course businesses like social media platforms.

Encryption, children and the State

Children who live under repressive regimes, whistleblowers and activists

In relation to the State, encryption plays a crucial role in securing the communications of children who would be targeted and subjected to violence by the government if the content of their searches or exchanges was revealed. This is particularly true for children who want to exercise their civil and political rights under repressive regimes, as the first scenario shows.

Scenario 1

Mahsa is a 16-year-old who lives in a country known for the violent excesses of its morality police. She uses unencrypted social media platforms to organise a peaceful youth protest against police brutality. The government has been monitoring communications on these platforms, finds out about the protest and forcefully disperses it. Police and security services use data monitored across unencrypted platforms to identify people who attended or were involved in planning the protest. Mahsa and other children are arrested, severely beaten and prosecuted.

222 CRIN and ddm conversation with Data Privacy Brazil Research Association, 24 November 2022.

While this scenario is inspired by the 2022 Iranian protests which saw children being intimidated, arrested and killed,[223] impermissible restrictions on children's freedom of assembly have long been documented. In the wake of the Arab Spring, children who protested in Egypt have been jailed, tortured and murdered.[224] In Bahrain they were beaten and threatened with rape and electric shocks.[225] In Indonesia child protesters were arrested,[226] and in Thailand they were fired at.[227] In Myanmar they were met with brutal crackdowns.[228] Intimidations have been reported even in countries with generally strong protection of political rights and civil liberties[229] - in the UK, for example, police were accused of deploying tactics meant to deter children from protesting against climate change.[230]

These examples show that children can be at serious risk of physical harm from the State if they do not have the means to communicate securely in order to exercise their rights. In these cases, the privacy afforded by encryption also serves children's right to protection from violence.

Encryption also has disproportionate benefits for children who might not be directly at risk of physical violence, but whose rights are threatened by regimes which practise surveillance and censorship.

223 Human Rights Watch, *In Iran, Schoolgirls Leading Protests for Freedom*, 12 October 2022, https://www.hrw.org/news/2022/10/12/iran-schoolgirls-leading-protests-freedom

224 The Nation, *The Children of the Arab Spring Are Being Jailed and Tortured*, 18 September 2017, https://www.thenation.com/article/archive/the-children-of-the-arab-spring-are-being-jailed-and-tortured

225 Human Rights Watch, *Bahrain: Police Beat, Threaten Children*, 10 March 2021, https://www.hrw.org/news/2021/03/10/bahrain-police-beat-threaten-children

226 UNICEF, *UNICEF calls for the protection of children involved in Indonesia's protests*, 1 October 2019, https://www.unicef.org/press-releases/unicef-calls-protection-children-involved-indonesias-protests

227 Amnesty International, *Thailand: Urgent investigation needed after live rounds fired at child protesters*, 18 August 2021, https://www.amnesty.org/en/latest/news/2021/08/thailand-urgent-investigation-needed-after-live-rounds-fired-at-child-protesters/

228 The Guardian, *Fear turns to fury in Myanmar as children shot by military*, 28 March 2021, https://www.theguardian.com/global-development/2021/mar/28/fear-turns-to-fury-in-myanmar-as-children-shot-by-military

229 See, for example: Freedom House, *Freedom in the World 2022*: United Kingdom, https://freedomhouse.org/country/united-kingdom/freedom-world/2022

230 Manchester Evening News, *Greater Manchester Police are collecting evidence against children protesting about climate change and threatening them with arrest*, 28 June 2019, https://www.manchestereveningnews.co.uk/news/greater-manchester-news/greater-manchester-police-collecting-evidence-16481957

Scenario 2

Xiu is 15 and lives under a regime where cyber-censorship is widely practised. In order to circumvent censorship, critics of the regime have been using the name and image of a cartoon character to make reference to the country's leadership.[231] Xiu tries to use these references to read the writings of activists and communicate with other like-minded people. Her searches and messages are scanned and blocked.[232]

This scenario shows how the lack of encryption can put at risk children's right to seek, receive and share information, as well as express themselves on a variety of topics of concern to them. Some States, such as China through its Great Firewall,[233] have created complex systems of online censorship, which directly threaten children's rights. A field experiment with Chinese university students on the effects of providing access to an uncensored Internet found that "modest and temporary incentives to visit Western news outlets led to a persistent increase in students' acquisition of politically sensitive information", and that the "acquisition of politically sensitive information brings broad, substantial and persistent changes to students' knowledge, beliefs, attitudes and intended behaviours", for example discussing political topics with others.[234]

Freedom of expression and information is particularly important in the current political context, where authoritarianism is on the rise. Some experts fear that "the global order is nearing a tipping point" and that if freedom is not guaranteed, "the authoritarian model will prevail".[235] And "freedom of expression is the first right authoritarian leaders attack as they move to undermine democracy" because "the defining battle for power is a battle to control the narrative."[236] The importance of encryption becomes apparent in a world where over a third of the population live in countries which are "not free"[237] or where freedom of expression is "in crisis".[238]

231 This scenario was partly inspired by: BBC, *Why China censors banned Winnie the Pooh*, 17 July 2017, https://www.bbc.co.uk/news/blogs-china-blog-40627855

232 See, for example: The New York Times, *Apple's Compromises in China: 5 Takeaways*, 17 May 2021, https://www.nytimes.com/2021/05/17/technology/apple-china-privacy-censorship.html

233 See, for example: TechTarget, *Great Firewall of China*, https://www.techtarget.com/whatis/definition/Great-Firewall-of-China

234 Chen and Yang, *The Impact of Media Censorship: 1984 or Brave New World?*, American Economic Review 2019, 109(6): 2294–2332, pp. 2995-2996, https://www.gwern.net/docs/sociology/2019-chen.pdf

235 Freedom House, *Freedom in the World 2022: The Global Expansion of Authoritarian Rule*, https://freedomhouse.org/report/freedom-world/2022/global-expansion-authoritarian-rule

236 ARTICLE 19, *The Global Expression Report 2022: The intensifying battle for narrative control*, June 2022, p. 6, https://www.article19.org/wp-content/uploads/2022/06/A19-GxR-Report-22.pdf

237 Freedom House, *Freedom in the World 2022: The Global Expansion of Authoritarian Rule*.

238 ARTICLE 19, *The Global Expression Report 2022: The intensifying battle for narrative control*, June 2022, p. 5.

Regarding children who are part of specific groups, encryption is important for protecting their safety where belonging to disadvantaged or marginalised communities exposes them to state violence, as the following scenario shows.

Scenario 3

Amadou is a gay 17-year-old. In his country homosexuality is illegal and stigmatised, and members of the LGBT+ community regularly face violence from the state and the public. Amadou uses unencrypted messaging services to meet with other LGBT+ youth and share information about sex education. The police intercept these communications and Amadou is arrested on homosexuality charges. Police then use Amadou's contacts to identify and target other LGBT+ young people.[239]

Encryption poses particular benefits to LGBT+ young people from countries (for example, the United Arab Emirates) which criminalise homosexuality, block LGBT-related content, and monitor chat rooms, instant messages, and blogs.[240] At the same time, child protection advocates have emphasised that evidence suggests that children who identify as LGBT+ and/or disabled are more likely to experience online sexual harms during childhood,[241] with LGBT+ young people being pressured into sharing sexual images more than their heterosexual peers.[242]

Where children from disadvantaged or marginalised groups want to blow the whistle on the systemic abuse they are subjected to, encryption can play a relevant role, as the next scenario shows.

Scenario 4

Ishaan, a 15-year-old with a disability, attends a "special school" where he is constantly bullied, including by school staff.[243] He writes a damning piece which reveals the abuse suffered by himself and other children in his school, and criticises the government for their policies. He sends the piece to various people, including a journalist, via direct message. They all forward it on different platforms. The story becomes viral, but the journalist refuses to name his source. However, the government has in place a "traceability" law which requires electronic service providers to be able to identify the originator of a certain message.

239 This scenario was partly inspired by: Human Rights Watch, *Cameroon: Wave of Arrests, Abuse Against LGBT People*, 14 April 2021, https://www.hrw.org/news/2021/04/14/cameroon-wave-arrests-abuse-against-lgbt-people

240 VPN Overview, *Censorship in the UAE: How to Get Around it*, updated on 16 November 2022, https://vpnoverview.com/unblocking/censorship/internet-censorship-uae/

241 WeProtect Global Alliance, *Global Threat Assessment 2021*, p. 18.

242 Id., p. 56.

243 This scenario was partly inspired by: The Guardian, *Children with disabilities suffer 'severe neglect and abuse' in Australian schools*, 27 October 2019, https://www.theguardian.com/society/2019/oct/28/children-with-disabilities-suffer-severe-neglect-and-abuse-in-australian-schools

Digital privacy advocates[244] and providers of end-to-end encrypted services[245] have warned that traceability provisions undermine the privacy and security guarantees of end-to-end encryption. They argue that, since it is not possible to know in advance which messages governments would want to trace, traceability provisions in effect mandate that messaging services, through logs of metadata, keep track of who sent something to whom and when for every message. They also caution that these provisions are not effective, since the originator and the creator of content might not be the same person - for example, if a person simply downloads an image and then shares it, they would be considered an originator of that image.[246]

But end-to-end encryption remains critical for children who want to expose injustice. As Edward Snowden put it simply, "It would have been impossible for me to whistleblow without encryption".[247]

Children who make decisions about their own body

Even where children do not take part in activism but simply want to make decisions regarding their own body, for instance, the State can interfere in ways that put many of their rights at risk. Encryption therefore becomes relevant to protect those rights, as the next example shows.

Scenario 5

Elena is 12 and becomes pregnant after a rape. Her country criminalises abortion and does not make exceptions for rape or incest. She uses unencrypted messaging apps to find a doctor that would perform an abortion in her country, and also searches online for abortion clinics in neighbouring countries. In order to collect criminal evidence, the government requests platforms to scan content for abortion-related language. It also monitors web searches and flags users looking at abortion-related material.

The debate on abortion rights has at its core the principle of bodily integrity. It is the idea that everyone, including children, has the right to autonomy and self-determination over their own body.[248] This principle is being disproportionately infringed in the case of children, who are more often than adults subjected to

244 See, for example: EFF, *Why Indian Courts Should Reject Traceability Obligations*, 2 June 2021, https://www.eff.org/deeplinks/2021/06/why-indian-courts-should-reject-traceability-obligations; Access Now, *10 facts to counter encryption myths*, August 2021, https://www.accessnow.org/cms/assets/uploads/2021/08/Encryption-Myths-Facts-Report.pdf

245 WhatsApp, *What is traceability and why does WhatsApp oppose it?*, https://faq.whatsapp.com/2566310993676701/?locale=en_US

246 Ibid.

247 Global Encryption Coalition, *Edward Snowden and the Global Encryption Coalition say "Meddling with strong encryption puts public and economy at risk"*, 21 October 2021, https://www.globalencryption.org/2021/10/edward-snowden-and-the-global-encryption-coalition-say-meddling-with-strong-encryption-puts-public-and-economy-at-risk-press-release/

248 CRIN, *Bodily integrity*, https://home.crin.org/issues/bodily-integrity

practices regarding their body which they do not consent to.[249] Unreasonable restrictions on abortion violate bodily integrity, and they also put at risk the general principles underpinning the CRC, from non-discrimination and best interests of pregnant children to their right to life and right to be heard in the matters which affect them. These restrictions also threaten a range of other children's rights, such as the right to health, freedom of information, privacy, freedom of thought, and the right to be free from mental violence.[250]

Although the Committee has urged States to decriminalise abortion to ensure that girls have access to safe abortion and post-abortion services,[251] abortion remains illegal or restricted in a number of countries around the world.[252] Encryption is therefore particularly important for pregnant under-18s who want to understand what options are available to them in order to exercise their right to make decisions over their own body, without fearing repercussions.

That encryption has very practical implications for pregnant children is proved by a case from the US, where it was reported that Facebook contributed evidence in an abortion prosecution, by handing over to the police unencrypted messages between a pregnant 17-year-old from Nebraska and her mother discussing abortion pills.[253] Especially in light of the decision by the US Supreme Court to overturn after almost 50 years the constitutional protection for abortion in *Roe v. Wade*,[254] many technology experts in the US and elsewhere have called on companies to limit the extent of data they collect and retain which might be used to ascertain information about users' reproductive health.[255] One of the ways platforms can minimise the amount of data they gather is by expanding end-to-end encryption.

Children disproportionately affected by general rights limitations under the law

More generally, the debate on encryption, children and the State should also include a discussion of the restrictions on human rights that governments can place under international law and how the contours of these limitations might disproportionately affect children from particular communities, including in countries which do not necessarily bear the marks of authoritarianism.

249 Ibid.

250 For a discussion of other rights engaged, see: Human Rights Watch, *Q&A: Access to Abortion is a Human Right*, 24 June 2022, https://www.hrw.org/news/2022/06/24/qa-access-abortion-human-right

251 UN Committee on the Rights of the Child, *General comment No. 20 (2016) on the implementation of the rights of the child during adolescence*, CRC/C/GC/20, 6 December 2016, para. 60, https://www.refworld.org/docid/589dad3d4.html

252 Center for Reproductive Rights, *The World's Abortion Laws*, https://reproductiverights.org/maps/worlds-abortion-laws/

253 The Guardian, *Facebook gave police their private data. Now, this duo face abortion charges*, 10 August 2022, https://www.theguardian.com/us-news/2022/aug/10/facebook-user-data-abortion-nebraska-police

254 *Dobbs v. Jackson Women's Health Organisation* [US Supreme Court], No. 19–1392, decided 24 June 2022.

255 The Guardian, *Facebook gave police their private data. Now, this duo face abortion charges*, 10 August 2022.

Children's rights can be restricted under states of emergency. For example, the International Covenant on Civil and Political Rights provides that States can derogate from their human rights obligations if this is "strictly required" during an officially proclaimed "public emergency which threatens the life of the nation".[256] The COVID-19 crisis has already shown the dangers of States misusing emergency decrees to go beyond what is required to contain the spread of the pandemic and therefore permissible under law.[257]

Crucially, the derogations must not "involve discrimination solely on the ground of race, colour, sex, language, religion or social origin".[258] Therefore, where governments limit the use of encryption in the context of a state of emergency, the question of whether this discriminates against children from ethnic and linguistic minorities, for example, should be examined carefully, as the next scenario shows.

Scenario 6

Nina is a 16-year-old living in Country Urania, which neighbours Country Ruritania. Nina belongs to the Ruritanian ethnic minority. She is bilingual in languages Uranian and Ruritanian, as are a wide majority of Urania's citizens, but prefers to speak Ruritarian with her family. Ruritania invades Urania, to international shock and condemnation. The letter A becomes a symbol of the pro-Ruritanian forces. The Uranian government has declared a state of emergency, has banned end-to-end encryption and requires platforms to flag all users of the Ruritanian language who have shared images of the letter A. Nina shares in her family's group chat a picture of the letter A graffitied on a building, denouncing those who drew it. Nina's account is blocked and she is reported to the authorities.

Even where the situation does not rise to the level of state of emergency, the role of encryption should be discussed in the wider context of other State measures which limit fundamental freedoms. These restrictions might still threaten children's rights, for example freedom of information, and disproportionately affect those from particular communities, such as religious minorities, as the next scenario shows.

256 Art. 4, International Covenant on Civil and Political Rights.

257 See, for example: Special Rapporteurs and Independent Experts of the UN Human Rights Council, *COVID-19: States should not abuse emergency measures to suppress human rights – UN experts*, 16 March 2020, https://www.ohchr.org/en/press-releases/2020/03/covid-19-states-should-not-abuse-emergency-measures-suppress-human-rights-un; Kriszta Kovács, *Hungary's Orbánistan: A Complete Arsenal of Emergency Powers*, 6 April 2020, https://verfassungsblog.de/hungarys-orbanistan-a-complete-arsenal-of-emergency-powers/; Radosveta Vassileva, *Bulgaria: COVID-19 as an Excuse to Solidify Autocracy?*, 10 April 2020, https://verfassungsblog.de/bulgaria-covid-19-as-an-excuse-to-solidify-autocracy/. For a general discussion about COVID-19 and emergency powers, see: Cassandra Emmons, *International Human Rights Law and COVID-19 States of Emergency*, 25 April 2020, https://verfassungsblog.de/international-human-rights-law-and-covid-19-states-of-emergency/

258 Art. 4, International Covenant on Civil and Political Rights.

Scenario 7

Leila is 10 and a Muslim. She talks openly about her religion at school. When one of her schoolmates taunts her and mockingly calls her "jihadi bride", she wants to understand more about what this means and uses one of the school computers to search for the term. In her country, guidance from the Department for Education requires schools to have filters and monitoring systems in order to detect putative signs of "radicalisation". Her unencrypted searches are flagged,[259] and she is referred to the country's programme designed to stop people becoming terrorists or supporting terrorism.

One of the legitimate aims for which States can restrict some children's rights is the "protection of national security",[260] but this provision is susceptible to abuse by governments. In the UK, for instance, with regard to terrorism prevention, guidance provides for the monitoring of children's online searches, but says little about the protection of their privacy. If they are wrongly identified to be "at risk of radicalisation", children are referred to Prevent, a counter-terrorism programme which disproportionately targets Muslim children and poses serious risks to children's fundamental freedoms, some of its practices having been found to infringe their privacy and data rights.[261] Encrypted searches could therefore be one way of upholding the rights of children from religious minorities. At the same time, individuals and groups attempting to groom children and organise political violence use encrypted channels to do so. Policy discussions around the benefits and risks of encryption for children's rights need to take such specificities into account.

Encryption, children and their family

In the case of children and their family, the debate on the role of encryption should take into account at least two contexts which have received little attention so far: the case of children whose interests or views diverge from those of their parents, and that of children who might be put at a disadvantage due to the status of their parents.

The Committee has recognised that "[t]he digital environment presents particular problems for parents and caregivers in respecting children's right to privacy" and has specifically mentioned the risks posed by "[t]echnologies that monitor online activities for safety purposes".[262]

259 The term "jihadi bride" appears on the list of keywords that software could flag: The Guardian, *Schools monitoring pupils' web use with 'anti-radicalisation software'*, 10 June 2015, https://www.theguardian.com/uk-news/2015/jun/10/schools-trial-anti-radicalisation-software-pupils-internet

260 See, for example, Art. 13 of the Convention on the Rights of the Child.

261 For a discussion of Prevent and children's rights, including a particular focus on children's data, see CRIN, *Preventing Safeguarding: The Prevent strategy and children's rights*, March 2022, https://static1.squarespace.com/static/5afadb22e17ba3eddf90c02f/t/62385835c6d6f61c4977be26/1647859768092/Preventing+Safeguarding+March+2022+CRIN.pdf

262 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, para. 76.

It has also acknowledged that "[p]rotecting a child's privacy in the digital environment may be vital in circumstances where parents or caregivers themselves pose a threat to the child's safety".[263] The encryption debate should take this into account. As the next scenario shows, for example in cases of domestic violence, monitoring technologies can place children at risk.

Scenario 8

Cora, a 9-year-old, has a physically abusive mother. She does not tell this to any of her relatives, fearing that no one will believe her and that they will alert her mother. However, she takes photos of the bruises on her naked body to help evidence the abuse, and tries to send them to a friend whose family works for the police. The phone flags the photos and notifies her mother.

This example highlights how children who are victims of domestic violence could be put at risk by initiatives to scan the content on their phones for sexual abuse or signs of grooming, and then notify the parents. The automatic detection process might be overinclusive, because the necessary context, which would be more apparent to a human reviewer, is missing. Images could be flagged which might be evidence of violence, but which do not in fact indicate sexual abuse or grooming. Therefore the abusive parents might be alerted when children try to seek help and send evidence. This would put children at further risk of violence due to the potential for retaliation.

So secure communication is particularly important for children who are victims of domestic violence because it allows them to communicate securely with people outside the home whom they trust, for example in order to seek help. If children store and send evidence of abuse using encryption, the abusers cannot intercept it and tamper with it. This upholds children's privacy and protects them from physical and mental violence perpetrated by the abusers.[264]

Even if the parents do not necessarily represent a threat to their children, monitoring technologies can create difficulties for children, particularly if they start to develop views which are different from those of their parents, as the following scenario exemplifies.

263 Id., para. 77.

264 The importance of encryption for victims and survivors of domestic violence, sexual violence, stalking and trafficking is discussed in more detail here: ISOC, *Fact Sheet: Understanding Encryption: The Connections to Survivor Safety*, 18 December 2020, https://www.internetsociety.org/resources/doc/2020/understanding-encryption-the-connections-to-survivor-safety/

Scenario 9

Alex is 12 and comes from a very conservative family. Alex has been assigned female at birth. However, they have been questioning their gender identity for a while. Concerned about the changes their body is going through, they have started reading about ways to make it appear less feminine. One day, when their parents are not at home, Alex binds their chest and sends a photo to a friend they trust. Their phone flags the content as sexually explicit, and their parents are notified and receive a copy of the photo.[265]

The CRC states that parents have responsibilities, rights and duties to provide guidance to their children, "in a manner consistent with the evolving capacities of the child" (Art. 5). To the extent that children have the capacity to make decisions for themselves, these decisions must be respected. The Committee has specifically recognised that "[p]arents' and caregivers' monitoring of a child's digital activity should be [...] in accordance with the child's evolving capacities".[266]

Technologies that monitor children's communications place some children, for example those belonging to the LGBT+ community, in a difficult position. These technologies risk infringing children's privacy by outing them to their parents when they are not ready or willing to discuss their sexual orientation or gender identity. These children are also at heightened risk of violence and abuse, for example being kicked out of the home, if their parents are not accepting of their identity.[267] As with victims of domestic violence, end-to-end encrypted communication is therefore particularly important for LGBT+ children.

The debate on encryption and children's rights should also highlight a group of children that have received little attention so far: those who might suffer discrimination on the basis of who their parents are, as the following scenario explores.

265 This scenario is adapted from a hypothetical example given by Jillian York from the EFF. See The Center for Public Integrity, *Proposed iPhone protections could put LGBTQ youth at risk*, 24 September 2021, https://publicintegrity.org/inside-publici/newsletters/watchdog-newsletter/iphone-protections-lgbtq-youth/

266 UN Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, para. 76.

267 This point was made in: The Center for Public Integrity, *Proposed iPhone protections could put LGBTQ youth at risk*, 24 September 2021.

Scenario 10

Dev is 8 and the son of a single mother who is HIV-positive.[268] His mother uses unencrypted platforms to connect with others and share information about HIV prevention and treatment services. She does not disclose her condition for fear that she might lose custody of her son. The state makes efforts to track all HIV-positive people, including by monitoring communications on online platforms, and identifies Dev's mother. Dev's whole school finds out. His teacher makes him sit separately from his classmates, and several of his peers start to verbally abuse him.

The CRC recognises that children are in a particular position because their status is often associated with that of their parents. Art. 2 of the CRC prohibits discrimination on the basis of "the child's or *his or her parent's or legal guardian's* [emphasis added] race, colour, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth or other status". It also requires that the child be protected against "discrimination or punishment on the basis of the *status* [emphasis added], activities, expressed opinions, or beliefs of the child's parents, legal guardians, or family members."

The children of HIV-positive parents often face stigmatisation, discrimination and "are denied access to information, education, health or social care services or community life".[269] Therefore, they are at particular risk if the HIV-positive status of the parents is revealed when the parents are not able to use encryption to communicate securely.

Encryption, children and businesses

The debate on encryption and children's rights brings to the fore the importance of businesses like social media platforms and must take into account the contexts in which they play a disproportionate role. As the scenario below shows, for example, end-to-end encryption can pose serious risks to children's right to be protected from violence where influential encrypted platforms are being used to incite violence offline.

268 This scenario was partly inspired by: RAND Corporation, *How Parental HIV Affects Children*, 2009, https://www.rand.org/pubs/research_briefs/RB9372.html

269 UN Committee on the Rights of the Child, *General Comment No. 3 (2003): HIV/AIDS and the rights of the child*, CRC/GC/2003/3, 17 March 2003, para. 7, https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsiQql8gX5Zxh0cQqSRzx6ZeEf9bA8YygWAWhjeBgKhcc0njrT-tlx20RETRkrClf0qEtVlKxay%2FFwzytKp1XPhB%2F6joKO6UVePMIHldiwQtwk

Scenario 11

Sophia is 13 years old and belongs to an ethnic minority group that is constantly being targeted by hate speech on end-to-end encrypted social media platforms. As a result, there has been a substantial increase in the number of violent attacks against members of Sophia's ethnic group, and she becomes reluctant to express her own identity and opinions for fear of being subjected to abuse.

Businesses play a crucial part in the digital environment, but there are some political, social and economic contexts in which their influence is so significant that whether they are encrypted or not disproportionately engages children's rights. One of the best-known examples is the role of Facebook in Myanmar. Many saw Facebook as "the internet in Myanmar",[270] because of its primacy as a source of information and a way for the authorities to communicate with the public. However, in light of the violence which broke out against the minority Rohingya Muslims, a report by the independent international fact-finding mission on Myanmar, established by the UN Human Rights Council, found that Facebook has been "a useful instrument for those seeking to spread hate", and that its response has been "slow and ineffective".[271] A £150 billion class action suit by the Rohingya against the company alleges that its algorithms amplified hate speech against the minority group and there was a lack of investment in local content moderators who would understand the language and cultural context. It also accuses Facebook of failing to take down specific posts inciting violence, and failing to shut down accounts, groups and pages that were fomenting tension.[272]

It is worth underlining that all these problems were present in an environment that was not end-to-end encrypted. End-to-end encryption would make these issues even harder to tackle, as it removes platforms' ability to detect problematic content. This shows the disproportionate impact that encrypting influential platforms has on children's rights, especially where they belong to minority groups.

So far the main focus in the debate on encryption and children's rights has been on the content of the communications, rather than other data, such as children's current location, address, records of calls and texts, etc.[273] But access to metadata also requires attention, particularly in the context of business activities and children's rights. This is because, even if the content of the child's communications is end-to-end encrypted, companies can collect this data about children, use it and share it for profit.[274]

Beyond the business context, in any case, metadata too can be revealing, as was argued in the discussion about traceability provisions. As the scenario below shows, for example, it could be also used by perpetrators in a way that puts children at risk of violence.

Scenario 12

Juan is a 14-year-old Indigenous environmental activist. He is part of an unarmed group who patrols Indigenous land to ensure that armed groups do not trespass and plunder it.[275] A member of an armed group steals Juan's phone and uses unencrypted data about his previous locations to determine what route the Indigenous patrol will take next. The patrol is then violently ambushed by the armed group.

The terms of the debate on encryption and children's rights should therefore be widened to take into account not just the encryption of content, but also the encryption of metadata, and consider its implications in diverse contexts.

270 BBC, *Myanmar coup: How Facebook became the 'digital tea shop'*, 4 February 2021, https://www.bbc.co.uk/news/world-asia-55929654

271 Report of the independent international fact-finding mission on Myanmar, A/HRC/39/64, 12 September 2018, p. 14, https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf

272 The Guardian, *Rohingya sue Facebook for £150bn over Myanmar genocide*, 6 December 2021, https://www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence

273 Kardefelt-Winther, D. et al., *Encryption, Privacy and Children's Right to Protection from Harm*, 2020, UNICEF Office of Research – Innocenti Working Paper 2020-14, p. 7.

274 Ibid.

275 This part of the scenario was inspired by a real case: The Guardian, *Shock in Colombia over murder of 14-year-old indigenous activist*, 18 January 2022, https://www.theguardian.com/global-development/2022/jan/18/colombia-indigenous-activist-murdered-14-breiner-david-cucuname

Legislative proposals

In recent years there has been an increase in the number of proposals for legislation and other initiatives around the digital environment which impact encryption, often with the aim of keeping people safe.[276]

The UN Special Rapporteur on freedom of expression identified in 2018 a variety of trends in State restrictions on encryption.[277]

- Some have adopted criminal laws banning the use of encryption, like Iran has done through its Computer Crimes Act.
- Some, like Russia, have passed laws requiring registration and government approval of encryption tools.
- Some countries have put forward frameworks in order to provide law enforcement and security agencies with access to communications. For example, China's Cybersecurity Law requires network operators to give 'technical support and assistance' to public and national security organs. The UK's Investigatory Powers Act in 2016, supplemented by the secondary regulations in 2018, allows authorities to issue a "technical capability notice" to online services, which might compel them to build backdoors and remove end-to-end encryption. It has been dubbed "the Snoopers' Charter" by privacy campaigners and was described as "the most intrusive and least accountable surveillance regime in the West" by Edward Snowden in 2015.[278] Australia followed suit, passing the Assistance and Access Act 2018, which requires service providers to develop technical capability to assist law enforcement and intelligence agencies. A similar proposal in the US, the Lawful Access to Encrypted Data Act, was put forward in 2020.
- Other States have used encryption as justification to institute broad hacking regimes, or have required online services to store personal or sensitive data locally, including encryption keys.
- Yet others, like India and Brazil, have proposed traceability requirements, asking the service providers to be able to identify the original sender of a message.[279]

---

276 For an overview of recent regulatory discussions, see Tech Against Terrorism, *Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies*, 2021; For a global overview of the legal status of encryption, see Global Partners Digital, *World map of encryption laws and policies*, https://www.gp-digital.org/world-map-of-encryption/

277 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression as follow-up to the 2015 report on the use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age, A/HRC/38/35/Add.5, 13 July 2018, https://digitallibrary.un.org/record/1638475?ln=en

278 See his remarks on Twitter at: https://twitter.com/snowden/status/661950808381128704

279 See Tech Against Terrorism, *Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies*, 2021, pp. 33-34.

The first attempt at legislation for online safety came from Australia in 2015, with its Enhancing Online Safety Act. This was updated in 2021 by the Online Safety Act, which came into effect in January 2022.[280] It provides a set of Basic Online Safety Expectations for online services that make them accountable for users' safety. It also requires industry to develop mandatory codes for illegal and restricted content, which can require platforms to remove child sexual abuse material and put greater pressure on online services to protect children from content which is not age-appropriate. The Act gives considerable power to the eSafety Commissioner, who can impose standards for the industry if no agreement is reached on the codes or if the standards developed are not appropriate.

Arguably, 2022 has been the most important year so far for regulatory discussions about protecting children online, particularly from sexual abuse and exploitation. Three proposals were put forward and are currently under discussion in the US, UK and the EU. Their aims are uncontroversial, but the suggestions for keeping children safe and the impact these suggestions have on (end-to-end) encryption are giving rise to disagreements.

US Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2022 (EARN IT Act of 2022)[281]

Changes envisaged by the proposal	Areas of disagreement regarding encryption and children's rights
The EARN IT Act of 2022 was introduced in January. The original version of the bill had been set out in 2020. The Act creates the National Commission on Online Child Sexual Exploitation Prevention, whose purpose is to "develop recommended best practices" that platforms can choose to implement to "prevent, reduce and respond to the online sexual exploitation of children".[282]	The aim of the EARN IT Act of 2022 is to fight against the online sexual exploitation of children. However, there have been warnings that the Act threatens the privacy of all users, that it could lead to over-removal of content, and that it might make it more difficult to prosecute those who exploit children online.[283] There are concerns that the Act might impose, in effect, a monitoring obligation on platforms.
The Act also amends Section 230 of the Communications Act of 1934, the current regime for intermediary liability online.[284] Currently, Section 230 prevents platforms from being treated as the publisher or speaker of what users post online. No liability can be imposed under State law that is inconsistent with this section. However, under Section 230 platforms' immunity does not extend to federal criminal law regarding the sexual exploitation of children. It is a federal crime for platforms to knowingly possess or share child sexual abuse material.[285] Platforms are also required to report such material on their services that they know about.[286] The EARN IT Act removes platforms' immunity regarding the "advertisement, promotion, presentation, distribution, or solicitation" of child sexual abuse material in civil and criminal actions under State law.[287] However, none of the following three factors - that platforms use end-to-end or other encryption on their services, that they do not have the necessary information to decrypt a communication, or that they fail to take actions that would undermine their ability to offer end-to-end or other encryption - can be an "independent basis for liability". Courts can consider evidence regarding those three factors if it is otherwise admissible.[288]	This is because, even though under federal law the standard for liability is actual knowledge of child sexual abuse material, State laws might have a lower standard such as recklessness or negligence regarding its existence. So a platform that does not know about child sexual abuse material on its services might be liable under State law if it should have known or was negligent about the existence of this material. The concern is that claimants or prosecutors might argue, for example, that offering encryption services is not an independent basis for liability, but is one of the factors contributing to the platform's reckless behaviour. Therefore, in order to avoid costly and lengthy litigation, platforms could be pressured to weaken or remove encryption from their services. They might also be incentivised to use client-side scanning to detect child sexual abuse material before the communication is encrypted or after it is decrypted. Critics also warn that the Act would deputise platforms as agents of the government, making the evidence they obtain inadmissible in court under the Fourth Amendment to the US Constitution, which prohibits the "unreasonable searches and seizures" of individuals' communications by law enforcement without a warrant.[289]

280 Australian eSafety Commissioner, *Online Safety Act 2021 - Fact sheet*, July 2021, https://www.esafety.gov.au/sites/default/files/2021-07/Online%20Safety%20Act%20-%20Fact%20sheet.pdf

281 Available at: https://www.congress.gov/bill/117th-congress/senate-bill/3538/text

282 Section 3 of the EARN IT Act of 2022.

283 See, for example: Riana Pfefferkorn, *The EARN IT Act Is Back, and It's More Dangerous Than Ever*, 4 February 2022, https://cyberlaw.stanford.edu/blog/2022/02/earn-it-act-back-and-it%E2%80%99s-more-dangerous-ever; Jeffrey Westling, *Unintended Consequences of the EARN IT Act*, 23 February 2022, https://www.americanactionforum.org/insight/unintended-consequences-of-the-earn-it-act/

284 See under Title 47 of the US Code: 47 U.S.C. 230 (e), available at: https://www.law.cornell.edu/uscode/text/47/230

285 Section 2252A, available at: https://www.law.cornell.edu/uscode/text/18/2252A

286 Section 2258A, available at: https://www.law.cornell.edu/uscode/text/18/2258A

287 Section 5 of the EARN IT Act of 2022. It also authorises federal civil suits for conduct that violates Sections 2252 or 2252A of the US Code.

288 Section 5 of the EARN IT Act of 2022.

289 Available at: https://www.law.cornell.edu/constitution/fourth_amendment

UK Online Safety Bill[290]	
Changes envisaged by the proposal	**Areas of disagreement regarding encryption and children's rights**
The UK Government introduced the Online Safety Bill in the House of Commons in March 2022. It had proposed the draft bill in May 2021, following its response to the public consultation regarding the Online Harms White Paper from April 2019. In 2022, the UK Government invested £500,000[291] into the "No Place to Hide" campaign,[292] which asks social media companies to commit to rolling out end-to-end encryption only when "they have the technology to ensure children will not be put at greater risk as a result". The Online Safety Bill imposes duties of care on providers of user-to-user services and search services.[293] All these providers have a duty to address illegal content such as child sexual exploitation and abuse, by carrying out risk assessments and taking proportionate measures to effectively mitigate and manage the risk of harm to individuals.[294] For example, user-to-user services have a duty to prevent individuals from encountering child sexual exploitation and abuse content, minimise the time for which such content is present, and swiftly take it down where they become aware of it.[295] All such content that is detected must be reported to the National Crime Agency.[296]	The Online Safety Bill is intended to deliver the commitment to "make the UK the safest place in the world to be online", including for children.[297] Concerns around the Online Safety Bill centre on the fact that, in practice, it seems to impose a general monitoring obligation, even for providers of services that use end-to-end encryption. In order to comply with the risk assessment and content moderation duties, as well as with any requirements from Ofcom, service providers would need to scan all user content. The failure to distinguish between public platforms and private messaging services means that offering end-to-end encryption might violate the duties under the Bill.[298] Platforms might have to use client-side scanning before the communication is encrypted or after it is decrypted. More broadly, critics have warned that the Bill focuses too much on content moderation instead of tackling the business model of platforms (the monetisation of users' attention), deputises platforms to make determinations regarding the illegality of content, infringes users' freedom of speech and privacy by covering "harmful" content that is not illegal, and endangers the independence of Ofcom by giving too much power to the Secretary of State over the implementation of the Bill.[306] From a children's rights perspective, it is concerning that so much power lies with Ofcom, even though it does not have specific expertise in this area.
In addition, user-to-user services and search services that are likely to be accessed by children must carry out a children's risk assessment and take proportionate measures to protect children from content that is harmful to them.[299] This is to be defined by the Secretary of State in secondary legislation.[300] Ofcom, the UK's communications regulator, can impose a "proactive technology requirement" on a service for the purpose of complying with the illegal content duties and children's online safety duties.[301] Moreover, Ofcom can order a provider of services to use "accredited technology" to identify and swiftly take down child sexual exploitation and abuse content, whether communicated publicly or privately.[302] In deciding whether it is necessary and proportionate to order this, Ofcom must consider a number of factors, including the kind of service, its functionalities, its user base, the prevalence and dissemination of the content, the risk and severity of harm, the systems and processes used by the service to identify and remove the content, and the risks to users' freedom of expression and privacy.[303] Ofcom can request providers of services to give any information that Ofcom requires for exercising, or deciding to exercise, its functions.[304] It is a criminal offence to provide information which is encrypted such that Ofcom cannot understand it, where the intention is to prevent Ofcom from understanding that information.[305]	

290 Available at: https://bills.parliament.uk/bills/3137. The analysis is based on the text of the Bill as of 5 December 2022.

291 Computer Weekly, *Government funds charity campaign to warn big tech over the risks of encryption to children*, 19 January 2022, https://www.computerweekly.com/news/252512196/Government-funds-charity-campaign-to-warn-big-tech-over-the-risks-of-encryption-to-children

292 Available at: https://noplacetohide.org.uk/

293 See, for example, sections 2, 6, 7, 22, 23 of the Online Safety Bill.

294 See, for example, sections 8, 9, 24, 25 of the Online Safety Bill.

295 Section 9 of the Online Safety Bill.

296 Section 60 of the Online Safety Bill.

297 UK Government, *Online Safety Bill: factsheet*, last updated on 19 April 2022, https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet

298 See, for example: ARTICLE 19, *UK: Online Safety Bill is a serious threat to human rights online*, 25 April 2022, https://www.article19.org/resources/uk-online-safety-bill-serious-threat-to-human-rights-online/

299 See, for example, sections 10, 11, 26, 27 of the Online Safety Bill.

300 Section 54 of the Online Safety Bill.

301 Section 120 of the Online Safety Bill.

302 Section 106 of the Online Safety Bill.

303 Section 108 of the Online Safety Bill.

304 Section 87 of the Online Safety Bill.

305 Section 94 of the Online Safety Bill.

306 ARTICLE 19, *UK: Online Safety Bill is a serious threat to human rights online*, 25 April 2022.

EU proposal for a "Regulation laying down rules to prevent and combat child sexual abuse"[307]	
Changes envisaged by the proposal	**Areas of disagreement regarding encryption and children's rights**
The EU proposal for a Child Sexual Abuse Regulation ("CSAR") was put forward in May 2022. The EU CSAR was developed in the context of the EU strategy for a more effective fight against child sexual abuse, which was adopted in July 2020.[308] It provides a framework for developing a comprehensive response to online and offline child sexual abuse. The strategy sets out various initiatives, including ensuring the complete implementation of the current legislation like the Child Sexual Abuse Directive,[309] identifying gaps and proposing new legislation, strengthening law enforcement and prevention efforts, and creating a European centre to prevent and counter child sexual abuse. In November 2020, the Council of the EU issued a resolution on "Security through encryption and security despite encryption".[310] In July 2021 the EU adopted a temporary derogation from the ePrivacy Directive,[311] allowing service providers to take voluntary measures to detect, report and remove child sexual abuse material. In October 2022, the EU adopted the Digital Services Act,[312] amending a 20-year-old directive[313] which applies to online services.	For background, there is a complex landscape regarding the approaches of the various EU initiatives and laws to end-to-end encryption. The EU strategy for a more effective fight against child sexual abuse acknowledges the use of encryption for criminal purposes and calls for "possible solutions which could allow companies to detect and report child sexual abuse in end-to-end encrypted electronic communications".[314] The EU Council Resolution on Encryption refers to "technical solutions for gaining access to encrypted data", noting that they should respect the "principles of legality, transparency, necessity and proportionality including protection of personal data by design and by default". On the other hand, the text of the temporary ePrivacy derogation specifically states that nothing in it should be interpreted as "prohibiting or weakening end-to-end encryption".[315] The Digital Services Act retains the prohibition on general monitoring, meaning that service providers cannot be asked to monitor information transmitted or stored, or actively seek circumstances indicating illegality.[316]

307 Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN

308 Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:607:FIN

309 Directive 2011/93/EU, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02011L0093-20111217

310 Available at: https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf

311 Regulation (EU) 2021/1232, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1232

312 Regulation (EU) 2022/2065, available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj

313 Directive on electronic commerce or E-Commerce Directive 2000/31/EC, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031

314 Introduction to the strategy.

315 Recital 25 of the temporary derogation.

316 Art. 8 of the Digital Services Act.

The EU CSAR sets out rules to address "the misuse of relevant information society services for online child sexual abuse".[317] These services are defined as: hosting services, interpersonal communications services, software applications stores, and internet access services.[318] The CSAR imposes risk assessment, mitigation and reporting obligations on hosting and interpersonal communication services regarding online child sexual abuse. This covers the "dissemination of material previously detected and confirmed as constituting child sexual abuse material ('known' material), but also of material not previously detected that is likely to constitute child sexual abuse material but that has not yet been confirmed as such ('new' material), as well as activities constituting the solicitation of children ('grooming')".[319] When carrying out a risk assessment regarding online child sexual abuse, among other factors, services must take into account various functionalities to address the risk such as prohibitions and restrictions laid down in terms and conditions and ways to enforce them, age verification and reporting tools.[320]	The EU Parliament had approved language protecting end-to-end encryption, but this did not make it in the final version of the Digital Services Act.[321] With regard to the EU CSAR itself, some EU authorities and civil society organisations have warned that the proposal poses risks to encryption and fundamental rights. Data protection bodies consider that the proposal raises "serious data protection and privacy concerns" and have called for it to be amended, "in particular to ensure that the envisaged detection obligations meet the applicable necessity and proportionality standards and do not result in the weakening or degrading of encryption on a general level".[322] Looking at communications around the proposal, such as the Impact Assessment and public statements from the EU Commission, it has been argued that end-to-end encryption would be a factor making a service risky. In order to mitigate the risk, services could feel pressured to remove encryption, or apply client-side scanning. This pressure will apply even without the services being subject to a detection order.[323]

317 Art. 1 of the CSAR.

318 Art. 2(f) of the CSAR.

319 Recital 13 of the CSAR.

320 Art. 3(2)(b) of the CSAR.

321 European Pirate Party, *Digital Services Act: Decision in part strengthens, in part threatens privacy, safety and free speech online*, 20 January 2022, https://european-pirateparty.eu/eu-parliament-adopts-dsa-position/

322 European Data Protection Board and the European Data Protection Supervisor (EDPB-EDPS), *Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*, 28 July 2022, https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf

323 EDRi, *Private and secure communications attacked by European Commission's latest proposal*, 11 May 2022, https://edri.org/our-work/private-and-secure-communications-put-at-risk-by-european-commissions-latest-proposal/

They must also consider the manner in which users use the service,[324] and in which the provider designed and operates the service.[325] Regarding the risk of solicitation of children, they must consider, for example, functionalities like enabling users to contact others directly and share images or videos with them, particularly through private communications.[326] Then, services must take mitigation measures to minimise the risk identified. These measures must be effective, targeted and proportionate, and they must be applied in a non-discriminatory manner, with due regard to consequences for fundamental rights.[327] They must also report the risk assessment and mitigation measures to the national Coordinating Authority.[328] The Coordinating Authority can request the competent national judicial authority to issue a detection order where there is a significant risk of the service being used for abuse, and the benefits of issuing the detection order outweigh the risks for the rights of all parties.[329]	Concerns have also been raised regarding the degree to which the EU Centre would actually be independent from Europol and law enforcement, with some fearing that the proposal in practice gives a mass surveillance mandate to a centralised police organisation.[330] Internal documents suggest that EU Member States are divided.[331] Austria, for example, voted on a binding resolution to reject the EU proposal in its current form, given the risk of a general monitoring obligation and how this threatens encryption and fundamental rights.[332]

324 Art. 3(2)(c) of the CSAR.

325 Art. 3(2)(d) of the CSAR.

326 Art. 3(2)(e)(iii) of the CSAR.

327 Art. 4(2) of the CSAR.

328 Art. 5(1) of the CSAR.

329 Art. 7(4) of the CSAR.

330 Centre for Democracy and Technology (Europe Office), *Briefing on Key Concerns Relating to a Proposal for Regulation laying down the Rules to Prevent and Combat Child Sexual Abuse (CSAM)*, 26 May 2022, https://cdt.org/wp-content/uploads/2022/06/CDT-Europe-Briefing-on-Key-Issues-in-CSAM-Proposal.pdf

331 Patrick Breyer MEP, *Chat control: Internal documents show how divided the EU member states are*, 15 September 2022, https://www.patrick-breyer.de/en/chat-control-internal-documents-show-how-divided-the-eu-member-states-are/

332 epicenter.works, *Chat control - a good day for privacy*, 3 November 2022, https://epicenter.works/content/chatcontrol-a-good-day-for-privacy

Services that receive detection orders must install and operate technologies that detect abuse,[333] which must be effective, sufficiently reliable, not able to extract any information other than that which is strictly necessary, and the least intrusive in terms of the impact on users' privacy, including the confidentiality of communication.[334] The EU CSAR also establishes the EU Centre on Child Sexual Abuse as an entity which is independent, although it relies on the support services of Europol. The EU Centre has a number of tasks, from facilitating the generation and sharing of knowledge and expertise to acting as a dedicated reporting channel for the EU, and in some circumstances conducting online searches for publicly accessible abuse material.[335]	

333 Art. 10(1) of the CSAR.

334 Art. 10(3) of the CSAR.

335 Arts. 40-50 of the CSAR.

A children's rights approach to encryption: Principles for policy-makers

The realisation of the full range of children's rights in digital environments is complex and nuanced. There are no one-size-fits-all solutions. This report sets out a principles-based set of recommendations for future regulation in ways that respect children's rights.

Challenges persist in upholding children's right to protection from violence in the digital environment, in the detection and reporting of content and action against perpetrators, as well as insufficient and inconsistent state support for the prevention of violence against children, assistance to victims and survivors and cross-border cooperation.

Where there is interference in children's behaviour and activity in a digital environment, including digital content access and/or content moderation whether encrypted or not then the law must be applied in a specific context and case, and its impact assessed both in terms of understanding the big picture at scale, and the specific incident.

An understanding of the functioning of encryption and the roles that it plays in the digital ecosystem is essential for effective and rights-respecting regulation. The different purposes of cryptography need to be understood in the context of where it is used in the digital environment, and its purposes.

Encryption cannot be addressed in isolation as a child protection issue, or placed in opposition to privacy and security but must be seen as a part of the systems in the digital environment. The digital environment itself forms part of the wider societal ecosystem. No single law or technological development can protect children online or secure their human rights in isolation. Each part of the wider societal ecosystem requires both proper investment and that we recognise any limitations. Attention should be paid to the wide range of actors that engage children in society, including law enforcement, health services, social services, schools and other institutions, and the role that each can and should play effectively and legitimately, their boundaries, and need for cooperation.

Framing and Process

1. **Actions affecting the digital environment must respect the full range of children's rights.**

   All interventions that affect the digital environment in general, and actions that engage encryption in particular, must respect the full range of children's rights, from protection from violence to privacy and freedom of expression.

   - **Privacy *and* protection:** Discussions should move beyond the dichotomy "privacy versus protection". All those involved in decision-making processes should recognise that all children's rights, including privacy and protection, are universal, indivisible and interdependent. This means that these rights apply to all children everywhere. There is no set of rights which is more important than others - all rights are equally important. These rights also support each other, with the fulfilment of each being necessary for the realisation of others.

   - **Child rights impact assessments:** All interventions that have a significant impact on children must be based on child rights impact assessments. This should involve pre-legislative scrutiny that assesses the impact of any law reform proposal on the full range of children's rights. Where an independent body is responsible for regulation, that regulator must include sufficient child rights expertise. Businesses with a significant impact on children's rights in this context should also conduct children's rights impact assessments, act on the outcomes of those assessments, and report on their implementation.

2. **Interventions engaging encryption must be seen within a wider ecosystem.**

   No single law, policy or technological development can protect children online or secure their human rights more broadly. Encryption cannot be addressed in isolation, but only as part of a wider ecosystem with a range of actors that can meaningfully interact, each with its own role that it can effectively and legitimately play.

   - **Start with the societal problem:** Encryption should not be the starting point in debates around societal problems affecting children. Instead, policy-makers should identify the policy goal to be achieved and consider the range of options, of a technological nature or otherwise, that could be implemented for this purpose. In assessing possible solutions, policy-makers should consider the variety of actors interacting in the societal ecosystem, including governmental agencies, law enforcement, health services, social services, schools, care centres and other institutions.

   - **Beware of techno-solutionism:** Policy-makers and other stakeholders should avoid relying on one-size-fits-all technological fixes. Decision-making should be based on a thorough understanding of the complex technological landscape, including in particular the multiple roles that encryption and other technologies play. Policies should be grounded in the reasonable capability of technology as it is, not as might be hoped for.

   - **Support the complete child protection ecosystem:** Child protection requires human trust and meaningful interaction across solid infrastructures for knowledge-sharing and intervention. To the extent that laws, policies and other initiatives already exist for the purpose of child protection, they should be fully implemented. There should be an emphasis on prevention and education, and appropriate funding should be provided to the wide range of services interacting in the ecosystem, from law enforcement and the justice system, to social services and victim support. Particular emphasis should be given to staff training, which should include, where appropriate, digital evidence management, analysis and practice, in order to promote the investigation and prosecution of the perpetrators of technology-enabled violence against children. Physical and mental health support services for child and adult victims and survivors of child sexual exploitation and abuse must be a priority. The need for a multidisciplinary approach to protection should be emphasised in order to break down barriers to cooperation between disciplines and professionals.

3. **All those with relevant expertise must be involved.**

   All professionals with relevant knowledge must be able to engage in discussions and decision-making regarding children and the digital environment, including on encryption. They must be able to do so on an equal footing and in an environment of mutual respect. Conversations must include specialists working on child protection, technology and Internet regulation, data protection and privacy, as well as participants with more generalist expertise in children's rights, human rights and digital rights. The views of civil society, academia, government, law enforcement and the business sector must be taken into account. Particular efforts should be made to include those working outside currently dominant Anglo- and Euro-centric spaces.

   - **Language:** There should be a recognition of the extreme sensitivity of aspects of the debate around encryption and children's rights, particularly as regards online child sexual exploitation and abuse. Those involved in discussions should exercise empathy and pay special attention to the framing and language used, as well as the expectations that are being created for victims and survivors of abuse.

   - **Data:** Emphasis should be placed on the importance of accurate data, in particular about the scale of abuse and the accuracy of content-detection

technologies. All participants to discussions should strive to fully explain the ways in which they use data in support of their arguments, in order to help disaggregate between the various causes of problems and move the debate on solutions forward.

4. **Children and other directly affected communities must be heard and their views given due weight.**

   Children's right to have their voices heard and given due weight must be upheld in all decision-making processes which concern them. Other directly affected communities, such as the adult victims and survivors of child sexual exploitation and abuse or those disproportionately affected by policing, surveillance, intelligence gathering or other intrusive data practices, must also be meaningfully included in these processes. Assumptions should not be made about the outcomes these groups may want. Not all children or members of a community have the same experiences, views or concerns. Decision-making processes should therefore aim to include diverse voices.

5. **Policy-makers engaging with encryption must address the impact beyond their own jurisdiction.**

   The digital environment is interconnected and regulation in one jurisdiction is very likely to cause ripple effects in others, or even globally. Policy-makers must work to understand these links, including by engaging in conversations with those working in different jurisdictions, especially where they are not part of the dominant Anglo- and Euro-centric debates.

Substance

6. **There should be no generalised ban on encryption for children.**

   If encryption were removed from all services that children use, far from protecting them, this would leave them vulnerable to a wide range of exploitation and abuse. It is possible to regulate the applications of encryption, however this must be consistent with children's rights.

7. **Interventions engaging encryption must be context-specific.**

   Measures should be tailored to the diverse experiences of children as full rights-holders, including children from disadvantaged and marginalised groups. Interventions must consider and address specific political, economic, social and cultural contexts and the varied ways in which children relate to the State, businesses, and their community and family.

- **Real-world uses of the digital environment:** Those involved in decision-making should promote a better understanding of the variety of real-world uses of the digital environment, including communications involving medical information, legitimate political organisation in repressive environments, or the routine reliance on particular platforms where there is limited accessibility to other services. More efforts should be made to include perspectives which are not necessarily consistent with the expectations of those within the Anglo- and Euro-centric contexts.

- **The repurposing of technology:** There should be a recognition that technologies for content detection in the digital environment can be repurposed. The nature of the content that needs to be identified is not technology-specific, but policy-specific. Tools used to detect illegal content, such as child sexual abuse material, could also be deployed to identify legitimate content and infringe the rights of those accessing it.

8. **Measures engaging encryption must be legal, necessary and proportionate.**

   Interventions engaging encryption should respect the principles of legality, necessity and proportionality. These principles apply to the content of communications, but also to the collection, sharing and retention of metadata. Measures should be provided for by law and should be sufficiently clear and precise. They should be limited to achieving a legitimate policy goal and should be the least intrusive way of doing so. Interventions must be necessary and proportionate limitations on children's qualified rights such as privacy, therefore they must strive for a high degree of specificity, instead of applying indiscriminately.

9. **Policy-making should address the role of business.**

   Regulation and policy should mandate more transparency around how platforms prevent and remedy violations of children's rights, including by requiring clear, accessible and child-friendly terms of service. Platforms should receive guidance on how to improve the design of services, especially user reporting for children. Businesses whose activities have a significant impact on children's rights should be encouraged to invest in researching, developing and sharing findings on new technologies, as well as in supporting the efforts of others working in this area.

   - **Reporting to authorities:** Where businesses obtain knowledge of the existence on their services of illegal content such as child sexual abuse material or illegal activity such as violence against children, they should take action under their terms of service, and expeditiously report this to law enforcement or other appropriate authorities.

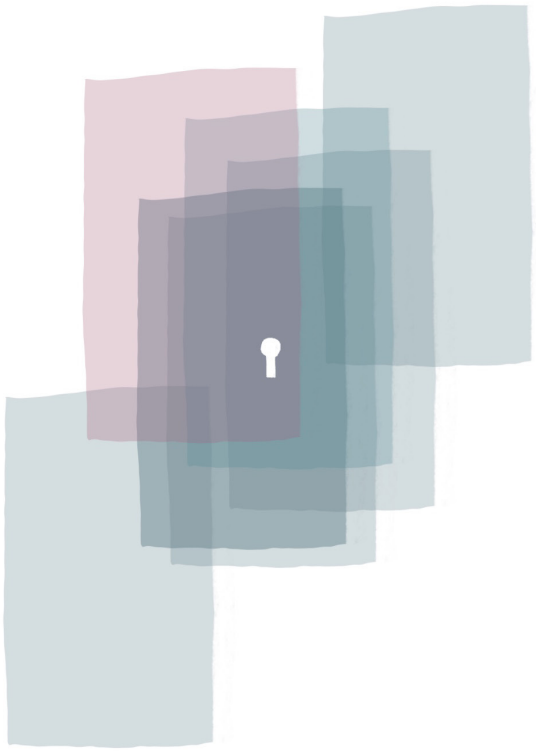
- **Transparency:** Companies should publish transparency reports regarding the scale of online child sexual exploitation and abuse on their services that comes to their knowledge, detailing the types of content and behaviour identified and the actions taken as a result. Efforts should be made to reach as much specificity as possible, disaggregating events into individual instances of abuse, analysing the prevalence of revictimisation through the sharing of identical or altered content, and indicating the context in which the events took place if relevant for ascertaining the intention of the users involved (e.g. consensual image sharing between children, or content shared in outrage).

10. Children must have access to justice.

Free, effective and child-friendly complaint mechanisms, both judicial and non-judicial, must be in place to ensure that children are able to access remedies, in a timely manner, for all violations of their full range of rights in the digital environment. There must be independent oversight mechanisms to ensure the lawful and rights-respecting implementation of measures engaging encryption.

- **User reporting:** Confidential, safe and child-friendly user reporting tools should be made available to ensure that children are able to report material and behaviour on services they use, and seek action. "Trusted flagger" mechanisms should also be considered. The decision following user reporting should be made in a timely manner, and it should be based on a clear and transparent process, giving users the possibility to resort to appeal mechanisms. Transparency reports should be produced to enable the scrutiny of systemic policy and practice around user reporting, while protecting the rights of users, as well as victims and survivors.

- **Content detection accuracy:** An overreliance on automated tools risks errors in the detection process and the wrongful removal of content, as well as other potential negative consequences such as the banning of users' accounts. Automation may support but cannot replace human content moderation. Any inadvertent outcomes due to errors from automated processes must be reversible through human support.



CRIN CHILD RIGHTS INTERNATIONAL NETWORK

defend|digital|me