Privacy *and* Protection:

A children's rights approach to encryption

Executive summary

CRIN CHILD RIGHTS INTERNATIONAL NETWORK

defend|digital|me

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

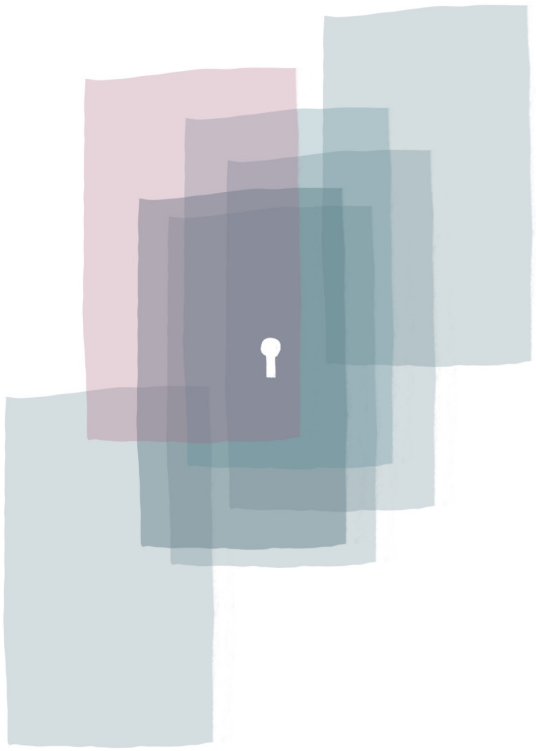
6. **There should be no generalised ban on encryption for children.**

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.



CRIN CHILD RIGHTS INTERNATIONAL NETWORK

defend|digital|me