Call for input to the High Commissioner's report on "the right to privacy in the digital age"

Global Encryption Coalition Steering Committee submission
June 2022

About the Global Encryption Coalition

The Global Encryption Coalition (GEC) was launched in 2020 to promote and defend encryption in key countries and multilateral fora where it is under threat. It also supports efforts by companies to offer encrypted services to their users. With more than 180 members from across the world, the Coalition is led by a steering committee made up of three global organisations: the Internet Society (ISOC), Global Partners Digital (GPD) and the Center for Democracy and Technology (CDT). GEC Members and Friends of the Coalition support the GEC's founding statement:

Encryption is a critical technology that helps keep people, their information, and communications private and secure. However, some governments and organisations are pushing to weaken encryption, which would create a dangerous precedent that compromises the security of billions of people around the world. Actions in one country that undermine encryption threaten us all. As a global coalition, we call on governments and the private sector to reject efforts to undermine encryption and pursue policies that enhance, strengthen and promote use of strong encryption to protect people everywhere. We also support and encourage the efforts of companies to protect their customers by deploying strong encryption on their services and on their platforms.[1]

We welcome the opportunity to respond to the Office of the High Commissioner for Human Rights' call for input to inform the development of the upcoming thematic report on the right to privacy in the digital age. In this joint response, the Steering Committee share insights on a number of the issues set out in the consultation as they relate to encryption. We draw on our expertise and ongoing engagement on these issues.

Encryption and the right to privacy

The important role of encryption in promoting and protection human rights has been recognised in Human Rights Council resolutions, UN General Assembly

[1] https://www.globalencryption.org/about/

resolutions and in the annual thematic reports of the Special Procedures of the Human Rights Council, including those of the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

For example, Human Rights Council resolution on "the promotion, protection and enjoyment of human rights on the Internet" (A/HRC/47/L.22) emphasises that "technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity, are important to ensure the enjoyment of all human rights offline and online".[2] Resolutions on the safety of journalists, including that one adopted by the Human Rights Council in 2020 (A/HRC/RES/45/18) emphasises that "that, in the digital age, encryption and anonymity tools have become vital for many journalists to exercise freely their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources".[3]

OHCHR's report on ways to bridge the gender digital divide from a human rights perspective states "Women's right to privacy in the context of equal access to ICTs implies the ability to benefit from encryption, anonymity or the use of pseudonyms on social media in order to minimize the risk of interference with privacy, which is especially pertinent for women human rights defenders and women trying to obtain information otherwise considered taboo in their Societies".[4]

In 2015, the Special Rapporteur for the right to freedom of expression, David Kaye's annual report (A/HRC/23/40) addressed the use of encryption and anonymity in digital communications. Drawing from research on international and national norms and jurisprudence, and the input of States and civil society, the report concludes that encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection. As noted in that report "encryption provides security so that individuals are able to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion"."[5]

In a follow up note to that report by the Secretariat in 2018, the mandate holder noted that "a number of developments have taken place, including a surge in State restrictions on encryption on the one hand, and increased attention to digital

[2] https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/47/L.22
[3] https://digitallibrary.un.org/record/3888335?ln=en
[4] https://digitallibrary.un.org/record/1298042?ln=en
[5] https://digitallibrary.un.org/record/798709?ln=en

security by key sectors of the ICT sector".[6] In that report he identified the following trends: Bans on Use and Dissemination of Encryption Tools; Licensing and Registration Requirements; Intentional Weakening of Encryption; Government Hacking; Mandatory Data Localization and Key Escrows and Restrictions on Encryption Tools Designed to Protect Anonymity.

Since then, these trends have continued, with legislative proposals that weaken encryption, mandatory data localisation and restrictions on tools designed to protect anonymity increasing in number. These challenge the development and continued use of end-to-end encryption and are emerging in many countries and regions.

Trends in encryption and implications for the right to privacy

Increasingly, governments are putting in place, or are proposing, measures that require large tech companies to be able to read, understand, filter, control, and report private communications they carry. These proposals often contend to address legitimate concerns of governments, particularly in addressing for example harms arising from the spread of disinformation, child sexual abuse material and the use of the internet to commit serious crimes. However, the undermining of encryption that would result and would impact all users and their rights present a disproportionate response. Though these proposals are often obscured in legislative proposals and sometimes referred to as technical means to enforce "legitimate law enforcement access" to data, such requirements are fundamentally inconsistent with end-to-end encryption. The very promise of that technology is that only the sender and the intended recipients are able to view the encrypted contents of a communication. Giving the provider — or other entities — access to this information runs afoul of the promise.

For example, in 2020 The Lawful Access to Encrypted Data (LAED) Act, S.4051 bill in the United States would have required that essentially forces companies to build backdoors to allow access to encrypted data even in contexts in which a warrant based on a finding of probable cause is not required.[7] Yet, as noted in a joint letter by members of the Global Encryption Coalition "The same backdoor placed in a system for use by law enforcement could be exploited by criminals, putting everyone on that service at greater risk of harm."[8] In the same year, the "Five-Eyes" intelligence alliance, plus India and Japan, called on companies to

---

6 https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf

7 https://www.congress.gov/bill/116th-congress/senate-bill/4051/text

8 https://www.globalencryption.org/2020/07/a-frontal-assault-on-encryption-by-mandating-backdoors/

create backdoors to their encrypted devices and services to provide law enforcement with exceptional access.[9]

In that year, an "EU strategy for a more effective fight against child sexual abuse material (CSAM)" and the proposals deriving from it, including the interim Regulation amending the ePrivacy Directive and the internal discussion document "Technical solutions to detect child sexual abuse in end-to-end encrypted communications" included proposals that would have undermined end-to-end encryption and put the right to privacy at risk. As noted in a letter by civil society sent in response to this paper "the Technical Solutions paper was technically flawed in at least two ways"[10]. First, it measured different technical solutions against "privacy," but failed to define the term. Second, the favoured solutions the paper identified all involve the result of law enforcement gaining exceptional access to content, while purporting to achieve the result that the recipient receives and decrypts a communication that was encrypted end-to-end. These two results are at odds: a service is not fully protected by end-to-end encryption unless only the sender and the recipient of a communication shared over the service can access its contents". As explained in a paper entitled "Breaking Encryption Myths"[11], authored by technical experts of the Global Encryption Coalition, "End-to-end encrypted communications cannot have exceptional access". In addition to analysing, and rejecting, client-side scanning and homomorphic encryption, the paper is a practical touchstone for why end-to-end encryption is incompatible with all content moderation techniques, because they must necessarily be complex, multi-stage and build in human oversight.

In 2021, the Indian government notified a new regime for intermediary liability that required law enforcement agencies can demand that companies trace the 'first originator' of any message.[12] This mandate required that communications be traceable to their origin so the purveyors of false information can be identified. However, as noted by Internet Society in their impact assessment of the regime "traceability of the first originator of certain information as well as users involved in a particular chain of messages infringes upon users' right to privacy and their right to anonymity."[13] Moreover "Rule 4(2) also gives access to law enforcement agencies, but is at risk of being exploited by state authorities to further surveillance, tracking political dissent and so on. This weakens security and privacy for all users who use end-to-end encrypted services and platforms."

---

[9] https://www.gp-digital.org/news/global-encryption-coalition-responds-to-new-statement-from-five-eyes/
[10] https://edri.org/wp-content/uploads/2020/10/20201020-EDRi-Open-letter-CSAM-and-encryption-FINAL.pdf
[11] https://cdt.org/insights/the-global-encryption-coalition-breaks-encryption-myths/
[12] http://egazette.nic.in/WriteReadData/2021/225464.pdf
[13] https://www.internetsociety.org/resources/2021/internet-impact-brief-2021-indian-intermediary-guidelines-and-the-internet-experience-in-india/

In the same year, reform of the Brazilian Code of Criminal Procedure included in articles 288 and 305 of the proposal impositions of duties on application providers to freely make available the technological means and resources necessary for interceptions to be carried out. As noted by signatories to a joint letter to the Brazilian Code of Criminal Procedure Reform Working Group "the text of the new CCP can legitimize government hacking practices and fishing expeditions. Generic language such as "remote collection", "resting data accessed from a distance", "forced computer system access", and "open source processing" can be responsible for facilitating access through surveillance technologies and can end up opening huge loopholes for uncontrolled abuses of state power, such as spying on journalists and activists, and for diminishing security and trust in computer systems". [14]

Later that year, a "Draft law on the collection and storage of identification, traffic and location data in the electronic communications sector and their access by the authorities"[15] was introduced in Belgium which would have required would require operators of encrypted systems to enable law enforcement to be able to access on request content produced by specific users after a specified date in the future. Yet, as stated in a letter sent by Global Encryption Coalition members to the Belgian government "There is no way to simply "turn off" encryption; providers would need to create a new delivery system and send targeted users into that separate delivery system. Not only would this require significant technical changes, but it would thereby break the promises of confidentiality and privacy of end-to-end encrypted communications services."[16] While it was eventually dropped, the proposal illustrates the continued trend in attempts to introduce backdoor access to encrypted data.

In the UK, the Online Safety Bill (2022) provides the UK communications regulator, OFCOM, with the powers to order a provider of a user-to-user service, which includes private messaging platforms, "to use accredited technology" to identify child sexual exploitation and abuse (CSEA) content, including on private messaging platforms.[17] However, in doing so, these notices could require that providers of such services introduce scanning capabilities into their platforms to scan all user content. Such scanning cannot be accomplished on end-to-end encrypted services for the simple reason that nobody, including the provider, has access to the content carried on that service except for the sender and the intended recipient(s). As a result, such a requirement could put users at risk by

[14] https://www.globalencryption.org/2021/06/brazilian-code-of-criminal-procedure-reform-must-not-undermine-encryption/
[15] https://www.brusselstimes.com/187667/privacy-group-calls-on-belgium-to-stop-trying-to-snoop-on-private-communications
[16] https://www.globalencryption.org/2021/09/open-letter-48-organizations-and-cybersecurity-experts-call-on-the-belgian-government-to-halt-legislation-to-undermine-end-to-end-encryption/
[17] https://bills.parliament.uk/bills/3137

compelling their service providers to compromise or abandon end-to-end encryption.[18]

Most recently, at the time of writing, the European Commission has proposed a Regulation that would require large tech platforms to detect, block, and report child sexual abuse information to a new clearinghouse (the EU Centre) that would in turn report the CSEA to Europol for enforcement.[19] Information that would have to be detected ranges from known CSEA images (detected through hashing technology), "new" CSEA images (detected through employment of AI tools) and "grooming" conversations, which would likely be detected through natural language processing tools that are notoriously inaccurate. A provider that abides by this obligation cannot offer an end-to-end encrypted service. [20]

Proponents of such mandates argue that client side scanning — which occurs on the user's device — can be used to detect such information consistent with end-to-end encryption. This is a myth, and nothing could be further from the truth. Once the scanning occurs and communications contents are accessed and are blocked or shared, end-to-end encryption is broken.[21]

Collectively, these examples point to worrisome trends that challenge the development and continued use of end-to-end encryption and which are emerging in many countries and regions. They implicate the human right to privacy because, in the modern day, encryption is critical to protecting, promoting and securing this right.

Conclusion

Governments should preserve and promote end-to-end encryption rather than compromise it, and should encourage companies to engage in other activities that protect end-to-end encryption while promoting solutions to address online harms and crimes that do not undermine user privacy and security. For example, with regards to addressing serious crimes like child sexual abuse material, they can encourage companies to facilitate the reporting of CSEA that their users encounter, and encourage the use of metadata analysis to detect CSEA activities.[22] They should actively engage with all stakeholders in the development of legislation and proposals to address online harms and crimes, in order to identify solutions that respect the right to privacy in the digital age.

---

[18] https://www.globalencryption.org/2022/04/45-organizations-and-cybersecurity-experts-sign-open-letter-expressing-concerns-with-uks-online-safety-bill/
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472
[20] https://www.globalencryption.org/2022/05/joint-statement-on-the-dangers-of-the-eus-proposed-regulation-for-fighting-child-sexual-abuse-online/
[21] https://www.globalencryption.org/wp-content/uploads/2020/11/2020-Breaking-Encryption-Myths.pdf
[22] https://cdt.org/insights/outside-looking-in-approaches-to-content-moderation-in-end-to-end-encrypted-systems/