

EXHIBIT 2



General Assembly

Distr.: General
4 August 2022

Original: English

Human Rights Council

Fifty-first session

12 September–7 October 2022

Agenda items 2 and 3

Annual report of the United Nations

High Commissioner for Human Rights and
reports of the Office of the High Commissioner
and the Secretary-General

Promotion and protection of all human rights, civil,
political, economic, social and cultural rights,
including the right to development

The right to privacy in the digital age

Report of the Office of the United Nations High Commissioner for Human Rights*

Summary

The present report, submitted pursuant to Human Rights Council resolution 48/4, discusses recent trends and challenges concerning the right to privacy. The report focuses, in particular, on: (a) the abuse of intrusive hacking tools; (b) the key role of encryption in ensuring the enjoyment of the right to privacy and other rights; and (c) wide-spread monitoring of public spaces. It highlights the risk of creating systems of pervasive surveillance and control that may undermine the development of vibrant and rights-respecting societies.

* Agreement was reached to publish the present report after the standard publication date owing to circumstances beyond the submitter's control.



intended target, its use should be limited to cases where it would serve to prevent or investigate a specific serious crime or act amounting to a grave threat to national security. Its use should be narrowly targeted to an investigation of the person or persons suspected of committing or having committed such acts. This should be a last resort, in other words, all less intrusive measures should have been exhausted or have been shown to be futile, and should be strictly limited in scope and duration. Only relevant data should be accessed and collected.³³ The measures should also be subject to rigorous independent oversight; prior approval by a judicial body is essential.³⁴ In addition, robust and transparent export controls that explicitly take into account human rights risks can be a powerful tool for preventing rights violations and abuses.³⁵ OHCHR reiterates its recent call as well as those of human rights experts and groups for a moratorium on the sale, transfer and use of hacking tools until a human rights-based safeguards regime is in place.³⁶

B. Restrictions on encryption

20. In recent years, various Governments have taken actions, which, intentionally or not, risk undermining the security and confidentiality of encrypted communications. This has concerning implications for the enjoyment of the right to privacy and other human rights.

21. Encryption is a key enabler of privacy and security online and is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly, security, health and non-discrimination. Encryption ensures that people can share information freely, without fear that their information may become known to others, be they State authorities or cybercriminals. Encryption is essential if people are to feel secure in freely exchanging information with others on a range of experiences, thoughts and identities, including sensitive health or financial information, knowledge about gender identities and sexual orientation, artistic expression and information in connection with minority status. In environments of prevalent censorship, encryption enables individuals to maintain a space for holding, expressing and exchanging opinions with others. In specific instances, journalists and human rights defenders cannot do their work without the protection of robust encryption, shielding their sources and sheltering them from the powerful actors under investigation. Encryption provides women, who face particular threats of surveillance, harassment and violence online, an important level of protection against involuntary disclosure of information.³⁷ In armed conflicts, encrypted messaging is indispensable to ensuring secure communication among civilians. It is notable that in the two months after the beginning of the armed conflict in Ukraine on 24 February 2022, the number of downloads in Ukraine of the encrypted messaging app Signal went up by over 1,000 per cent compared with preceding months.³⁸

22. The vital role of encryption as an enabler of privacy and human rights has been widely recognized, including by States, United Nations bodies, the United Nations High Commissioner for Human Rights and human rights experts.³⁹ The General Assembly and the Human Rights Council have also highlighted the importance of encryption in safeguarding human rights in several resolutions, calling upon States to refrain from interfering with

³³ See <https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf>.

³⁴ See A/HRC/39/29 on minimum safeguards for secret surveillance measures.

³⁵ A/HRC/39/29, para. 25; A/HRC/44/24, para. 40; A/HRC/48/31, para. 46; and A/HRC/41/35, paras. 34 and 66. The European Union recently took a step towards stronger human rights considerations by adopting a new export control regulation.

³⁶ See <https://www.ohchr.org/en/statements/2021/09/committee-legalaffairs-and-human-rights-parliamentary-assembly-council-europe>; <https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-lifethreatening>; <https://www.amnesty.org/en/documents/doc10/4516/2021/en/>; and <https://cyberpeaceinstitute.org/news/renewed-call-moratorium-spyware/>.

³⁷ A/HRC/35/9, para. 18.

³⁸ See <https://sensortower.com/blog/signal-telegram-ukraine-russia-2022>.

³⁹ See <https://www.ohchr.org/en/press-releases/2016/03/apple-fbi-case-could-have-serious-global-ramifications-human-rights-zeid>.

encryption technologies⁴⁰ and encouraging business enterprises to work towards enabling solutions to secure and protect the confidentiality of digital communications and transactions, including measures for encryption, pseudonymization and anonymity.⁴¹ Special rapporteurs and regional experts have expressed support for strong encryption as a rights enabler, recommending promoting and protecting strong encryption and cautioning against measures that would arbitrarily or unlawfully restrict the use of this key technology.⁴² The Committee on the Rights of the Child has underlined that any measures to detect child sexual exploitation and abuse material in encrypted communications must be strictly limited according to the principles of legality, necessity and proportionality.⁴³ The Human Rights Council, the United Nations and regional human rights experts have underscored that encryption is vital for journalistic work and the protection of sources.⁴⁴ The Internet Universality Indicators issued by the United Nations Educational, Scientific and Cultural Organization underscore the importance of encryption for trust and security online.⁴⁵

23. In spite of its benefits, Governments sometimes restrict the use of encryption, for example for the protection of national security and combating crime, in particular to detect child sexual abuse material. Restrictions include bans on encrypted communications and criminalization for offering or using encryption tools⁴⁶ or mandatory registration and licensing of encryption tools.⁴⁷ Similarly, in some instances, encryption providers have been required to ensure that law enforcement or other government agencies have access to all communications upon request, which can effectively amount to a blanket restriction of encryption that could require, or at least encourage, the creation of some sort of back door (a built-in path to bypass encryption, allowing for covert access to data in plain text).⁴⁸ Another form of interference with encryption is the requirement that key escrow systems be created and maintained, and all private keys needed to decrypt data be handed over to the Government or a designated third party.⁴⁹ The imposition of traceability requirements, according to which providers need to be able to trace any message back to its supposed originator, could also require the weakening of encryption standards.⁵⁰ Recently, various States have started imposing or considering general monitoring obligations for providers of digital communications, including those offering encrypted communications services.⁵¹ Such duties could effectively force those providers to abandon strong end-to-end encryption or to identify highly problematic workarounds (see paras. 27–28 below).

⁴⁰ General Assembly resolution 75/176, and Human Rights Council resolutions 39/6, 44/12, 45/18 and 48/4.

⁴¹ General Assembly resolution 75/176 and Human Rights Council resolution 48/4.

⁴² See A/HRC/29/32; <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf>; A/HRC/41/41; https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclaration10July2019_English.pdf; <https://www.osce.org/representative-on-freedom-of-media/379351>; and <https://www.eas.org/en/iachr/expression/reports/ENGIA2020.pdf>.

⁴³ Committee on the Rights of the Child, general comment No. 25 (2021) on children's rights in relation to the digital environment, para 70.

⁴⁴ Human Rights Council resolution 45/18; A/HRC/29/32; and <https://www.osce.org/representative-on-freedom-of-media/379351>.

⁴⁵ See <https://en.unesco.org/internet-universality-indicators>, indicator D.5.

⁴⁶ See PSE 2/2017 and LBY 3/2022. All communications mentioned in the present report are available from <https://spcommreports.ohchr.org/Tmsearch/TMDocuments>.

⁴⁷ See <https://hrsly.com/wp-content/uploads/2022/06/OL-L-BY-3-2022-DownloadPublicCommunicationFile.pdf> (LBY 3/2022).

⁴⁸ See GBR 4/2015, MYS 2/2018, AUS 5/2018 and AUS 6/2018.

⁴⁹ See RUS 7/2016 and RUS 7/2018.

⁵⁰ See IND 31/2018, IND 3/2019, BRA 6/2020 and BRA 7/2020.

⁵¹ For example, the "EARN IT" Act adopted in the United States of America in 2020 (see USA 4/2020); the draft Online Safety Bill in the United Kingdom (see GBR 5/2022); the European Commission proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 11 May 2022 (COM(2022) 209); and Government of India, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (see IND 8/2021).