United Nations A/HRC/51/17

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.

I. Introduction

1. The present report is submitted pursuant to Human Rights Council resolution 48/4, in which the Council requested the Office of the United Nations High Commissioner for Human Rights (OHCHR) to prepare a report identifying recent trends and challenges with regard to the human right to privacy and to identify and clarify related human rights principles, safeguards and best practices, and to present the report to the Council at its fifty-first session. The report reflects the responses received to the call for inputs issued by OHCHR.[1]

2. People around the world are witnessing impressive technological developments, as well as innovations that improve people's lives and boost economies. However, they are also experiencing how digital tools can be turned against them, exposing them to new forms of monitoring, profiling and control. Ensuring respect for and protection of the right to privacy, recognized in article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights and in many other international and regional human rights instruments[2] can play a central role in managing new digital threats to human rights, which are inextricably linked to the personal data that powers the engines of digitized societies.

3. Building on previous reports to the Human Rights Council addressing challenges to the right to privacy,[3] the present report focuses in on three notable trends relating to the role of States in safeguarding and promoting the right to privacy: (a) the widespread abuse of intrusive hacking tools; (b) the key role of robust encryption in ensuring the enjoyment of the right to privacy and other rights; and (c) the widespread monitoring of public spaces. The report highlights the very real and encroaching risk of creating systems of pervasive surveillance and control that may eventually choke the development of vibrant, prosperous and rights-respecting societies, concluding with a set of recommendations to avert such an outcome.

II. Surveillance of personal devices and communications

A. Hacking

4. In July 2021, Forbidden Stories, an investigative journalism consortium, supported by Amnesty International, published revelations about the use of Pegasus software that drew international attention to a human rights crisis that had been growing for years – namely the global proliferation of hacking tools for the targeted and covert surveillance of digital devices. While purportedly being deployed for combating terrorism and crime, such spyware tools have often been used for illegitimate reasons, including to clamp down on critical or dissenting views and on those who express them, including journalists, opposition political figures and human rights defenders.

5. The extent of Pegasus spyware operations and the number of victims are staggering. Based on a leaked list of over 50,000 phone numbers of potential and actual surveillance targets and a forensic analysis of numerous infected phones, reporting in 2021 revealed that at least 189 journalists, 85 human rights defenders, over 600 politicians and government officials, including cabinet ministers, and diplomats were affected as targets.[4] Investigations also exposed spying on judges, lawyers, doctors, union leaders and academics.[5] NSO Group,

[1] See https://www.ohchr.org/en/calls-for-input/2022/call-inputs-report-right-privacy-digital-age-2022.

[2] See article 16 of the Convention on the Rights of the Child; article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families; article 22 of the Convention on the Rights of Persons with Disabilities; article 10 of the African Charter on the Rights and Welfare of the Child; article 11 of the American Convention on Human Rights; and article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

[3] See A/HRC/27/37, A/HRC/39/29, A/HRC/44/24 and A/HRC/48/31.

[4] See https://www.washingtonpost.com/investigations/2021/07/24/whatsapp-pegasus-spyware/.

[5] See https://forbiddenstories.org/about-the-pegasus-project/; https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

the company that manufactures and sells Pegasus, has admitted that its customers target 12,000 to 13,000 individuals annually.[6]

6. Pegasus spyware is the most prominent example in a growing landscape of spyware marketed by companies to Governments across the globe.[7] According to researchers, at least 65 Governments have acquired commercial spyware surveillance tools.[8] NSO has reported that it counts 60 government agencies in 45 countries among its customers. Just days before the Pegasus revelations, Citizen Lab and Microsoft released a report that detailed how another software, Candiru, had been used by Governments to target human rights defenders, dissidents, journalists, activists and politicians.[9] In November 2021, the social networking company Meta announced that it had disabled seven entities that had targeted people through the Internet in over 100 countries. The company also alerted around 50,000 people whom it believed to have been targeted by such activities.[10] It has been reported that over 500 companies develop, market and sell such surveillance tools to Governments.[11]

7. The capabilities of spyware tools and services offered on the global market are formidable. Pegasus, for example, once installed, grants complete and unrestricted access to all sensors and information on infected devices, effectively turning most smartphones into 24-hour surveillance devices, accessing the camera and microphone, geolocation data, e-mails, messages, photos and videos, as well as all applications. It allows the intruder to obtain a detailed picture of the life of its victims, their thoughts, preferences, professional activities, political thinking, health, financial situation and social and intimate lives. While many hacking tools require some action on the part of the victim, such as clicking on a link or opening an attachment to a message, Pegasus is installed by stealth, through a so-called "zero-click attack".[12] The software makes it almost impossible for victims to avoid infection once they have been targeted.

8. Hacking operations can take many shapes with varying degrees of intrusiveness. While obtaining full control of a mobile phone or computer helps to draw a detailed picture of the lives of those targeted, a variety of other hacking techniques can be less intrusive, although still very serious, including obtaining access to e-mail accounts. Hacking can also access other connected devices, such as wearable technological devices or vehicles, which may provide additional information, including on health and location data. Devices equipped with cameras or microphones, such as smart speakers or television sets, can also be turned into audiovisual surveillance tools. Attacking the infrastructure of service providers can open access to vast amounts of information about thousands of customers, including their communications, browsing data and locations.[13] The discussion in the following paragraphs focuses on the hacking of personal communication devices.

---

[6] In testimony before the European Parliament, committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, 21 June 2022, available at https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20220621-1500-COMMITTEE-PEGA.

[7] See https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepressionReport2022_NEW_0.pdf, p. 29.

[8] See https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019.

[9] See https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/.

[10] See https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/. For other examples, see https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/; https://www.eff.org/press/releases/saudi-human-rights-activist-represented-eff-sues-spyware-maker-darkmatter-violating; and https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/.

[11] A/HRC/41/35, para. 6; see also https://data.mendeley.com/datasets/csvhpkt8tm/2 for a commercial spyware global inventory.

[12] It should be noted that Pegasus software is not the only tool with these capabilities and that the number of such tools is growing.

[13] The EncroChat investigation of the police in France and the Netherlands, which had managed to intrude the server infrastructure of an encrypted communications network, collected information about more than 32,000 phones in 121 countries; see German Federal Court of Justice, decision of 2 March 2022, 5 StR 457/21, para. 18.

9. The hacking of personal communication devices constitutes a serious interference with the right to privacy and can be linked to concerning violations of a range of other rights. Given that the intrusion into digital communication devices grants access to drafts and search and browsing histories, it may also permit deep insights into the thinking processes of the individuals subject to hacking, as well as their political and religious views and beliefs, thus interfering with freedoms of opinion and thought.[14] Hacking operations can be deeply traumatic experiences, affecting the mental health of the victims and their families. Hacking has reportedly led to the arrest and detention of human rights defenders and politicians, some of whom have reportedly been subjected to torture.[15] Targeted hacking has also been linked to extrajudicial killings.[16]

10. Moreover, targeting journalists and the media with hacking tools severely undermines media freedom not least because sources of information may fear detection and repercussions. The mere existence of hacking programmes can have chilling effects on freedom of expression, the work of the media and public debate and participation, potentially eroding democratic governance. In the words of the Supreme Court of India in its recent ruling on the use of Pegasus software, the chilling effect of surveillance would be an "assault on the vital public watchdog role of the press".[17]

11. Hacking may also have a negative impact on the rights to due process and fair trial.[18] Gaining access to a device can enable an intruder not only to observe the contents of that device and its interactions with other devices but also to manipulate the device, including by altering, deleting or adding files.[19] It is thus possible to forge evidence in order to incriminate or blackmail targeted individuals.[20]

12. Moreover, spyware may not only affect the targets of hacking operations but everyone in communication with those individuals, or, if the device's camera, microphone or geolocation is activated, any person present in the same physical location.[21]

13. Finally, hacking relies on and exploits the existence of security flaws in computer systems. By keeping such vulnerabilities open, or even creating them, those resorting to hacking may contribute to security and privacy threats for millions of users and the broader digital information ecosystem.[22]

14. Human rights bodies and experts have sounded the alarm about spyware for years. The General Assembly and the Human Rights Council have repeatedly stated that Member States should refrain from unlawful or arbitrary surveillance, including by way of hacking.[23] Several special rapporteurs have expressed strong criticism of hacking practices that go far beyond what is necessary to pursue legitimate objectives, such as countering terrorism and crime.[24] The Human Rights Committee has also expressed its concerns about State-sponsored hacking, in particular when employed without adequate oversight or safeguards.[25] At the

[14] A/HRC/29/32, para. 20. For a comprehensive analysis of freedom of thought, see A/76/380.

[15] See https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/.

[16] A/HRC/41/35, para. 1; see also the conference room paper of the Special Rapporteur on extrajudicial, summary or arbitrary executions, entitled "Annex to the report of the Special Rapporteur: investigation into the unlawful death of Mr. Jamal Khashoggi". Available from https://www.timesofisrael.com/nsos-pegasus-used-to-target-khashoggis-wife-before-his-murder-washington-post/.

[17] Supreme Court of India, *Manohar Lal Sharma v. Union of India*, order of 27 October 2021, para. 39.

[18] A/HRC/23/40, para. 62.

[19] A/HRC/39/29, para. 19.

[20] See https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/ for an example of such allegations.

[21] See https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, p. 8.

[22] A/HRC/39/29, para. 19.

[23] General Assembly resolution 75/176 and Human Rights Council resolutions 48/4 and 45/18.

[24] A/HRC/17/27; A/HRC/20/17; A/HRC/23/40, para. 62; A/HRC/41/35; A/HRC/41/41; and A/73/438; see also https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.

[25] See CCPR/C/DEU/CO/7; CCPR/C/NLD/CO/5; and CCPR/C/ITA/CO/6.

regional level, the former Special Rapporteur for freedom of expression of the Inter-American Commission on Human Rights condemned hacking operations for impermissible purposes and called for harsh punishments of offenders, including for actions taken for political reasons against journalists and the independent media.[26]

15. Reacting to the revelations about the use of the Pegasus software, various regional and national institutions, including the Council of Europe, the Inter-American Commission for Human Rights, the European Parliament and the Supreme Court of India, have expressed concerns about the proliferation of spyware and have initiated hearings and investigations.[27] Criminal investigations[28] and civil lawsuits[29] are also under way.

16. Guidance on minimum requirements and safeguards necessary for any governmental use of spyware can build on an extensive existing body of surveillance-related human rights analysis.[30] The far-reaching adverse impacts of hacking require a particularly cautious approach to its use, limiting it to the most exceptional circumstances, in strict adherence with the requirements of international human rights law.

17. However, many jurisdictions have not put such essential legal guardrails in place and do not have clear, precise, publicly available laws that govern hacking operations. While some States have enacted legal frameworks that would comply with international human rights law, others rely on overly broad or outdated laws enacted before the advent of modern technologies.

18. As the revelations about the Pegasus software and related reports have shown, hacking by various State actors often seems to pursue goals that are not legitimate under international human rights law. While, in certain circumstances, intrusive surveillance measures may be permissible under articles 17 and 19 of the International Covenant on Civil and Political Rights on grounds of the protection of national security or public order, hacking can never be justified for political or business reasons, which is often the case when human rights defenders or journalists are targeted.

19. Even if legitimate goals are being pursued, such as national security objectives or the protection of the rights of others, the assessment of the necessity and proportionality of the use of spyware severely limits the scenarios in which spyware would be permissible.[31] There are strong arguments that tools such as Pegasus, which enable unfettered intrusions into people's lives and can even reach into their inner thoughts, could affect the essence of the right to privacy[32] and interfere with the absolute rights to freedom of thought and opinion. Given the substantial adverse impacts of the use of spyware and its reach far beyond any

[26] See https://www.oas.org/en/iachr/expression/showarticle.asp?artID=998&lID=1.

[27] See https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1207&lID=1; https://www.oas.org/en/IACHR/jsForm/?File=/en/iachr/media_center/PReleases/2022/022.asp; https://www.theguardian.com/world/2022/mar/17/pegasus-spyware-ban-el-salvador-iachr-hearing; https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe; https://tvn24.pl/tvn24-news-in-english/polands-senate-lunches-special-committee-to-examine-use-of-pegasus-software-5557023; and Supreme Court of India, *Manohar Lal Sharma v. Union of India*, order of 27 October 2021.

[28] See https://www.euronews.com/next/2021/07/20/paris-prosecutor-to-investigate-alleged-pegasus-hacking-after-complaint-by-french-journali; and https://www.aljazeera.com/news/2021/7/22/hungary-prosecutors-open-investigation-into-pegasus-spying-claims.

[29] https://www.glanlaw.org/nso-spyware-hacking; https://privacyinternational.org/examples/2605/lawsuits-target-nso-group-selling-spyware-governments-targeting-activists-and; https://www.washingtonpost.com/technology/2021/11/23/apple-pegasus-lawsuit-spyware-nso/; and https://cdn.ca9.uscourts.gov/datastore/opinions/2021/11/08/20-16408.pdf. For an extensive overview of legal actions taken see https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/.

[30] See A/HRC/27/37; A/HRC/39/29; A/HRC/23/40 and A/HRC/23/40/Corr. 1; CCPR/C/UKR/CO/8; CCPR/C/DEU/CO/7; CCPR/C/ARM/CO/3; CCPR/C/BWA/CO/2; and CCPR/C/FIN/CO/7.

[31] See Federal Constitutional Court of Germany, judgment of 27 February 2008 (1 BvR 370, 595/07), at 247 (aa).

[32] European Data Protection Supervisor, see https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, p. 8.

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-legal-affairs-and-human-rights-parliamentary-assembly-council-europe; https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening; 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 technologies[40] 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 tools[46] 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.oas.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-LBY-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).

24. There is no doubt that widely used encryption capabilities, capabilities that the public has demanded as a response to mass surveillance and cybercrime, create a dilemma for Governments seeking to protect populations, in particular their most vulnerable members, against serious crime and security threats. However, as pointed out by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, regulation of encryption risks undermining human rights.[52] Governments seeking to limit encryption have often failed to show that the restrictions they would impose are necessary to meet a particular legitimate interest, given the availability of various other tools and approaches that provide the information needed for specific law enforcement or other legitimate purposes.[53] Such alternative measures include improved, better-resourced traditional policing, undercover operations, metadata analysis and strengthened international police cooperation.

25. Moreover, the impact of most encryption restrictions on the right to privacy and associated rights are disproportionate, often affecting not only the targeted individuals but the general population. Outright bans by Governments, or the criminalization of encryption in particular, cannot be justified as they would prevent all users within their jurisdictions from having a secure way to communicate. Key escrow systems have significant vulnerabilities, since they depend on the integrity of the storage facility and expose stored keys to cyberattacks. Moreover, mandated back doors in encryption tools create liabilities that go far beyond their usefulness with regard to specific users identified as crime suspects or security threats. They jeopardize the privacy and security of all users and expose them to unlawful interference, not only by States, but also by non-State actors, including criminal networks.[54] Licensing and registration requirements have similar disproportionate effects as they require that encryption software contain exploitable weaknesses.[55] Such adverse effects are not necessarily limited to the jurisdiction imposing the restriction; rather it is likely that back doors, once established in the jurisdiction of one State, will become part of the software used in other parts of the world.

26. Recently, the concept of so-called client-side scanning to detect certain forms of objectionable content has been proposed to avoid many of the problems outlined above. Client-side scanning moves the step of detection of content from the servers through which communications are sent to the personal devices themselves. In this way, content at issue is examined before being encrypted for transport. In August 2021, Apple announced plans to introduce such a system for its iMessage and iCloud services but suspended implementation of the proposed change after strong criticism from a broad range of information technology security experts, cryptographers and human rights groups.[56] However, various legislative attempts[57] may at least indirectly compel Internet communications services to implement such systems by imposing broad monitoring obligations for all communications, including those that are encrypted. Since the content of messages, once encrypted, cannot be accessed by anyone except the sender and the recipient, any general monitoring obligation would force service providers to either abandon transport encryption or seek access to messages before they are encrypted.

27. 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. Mandated client-side scanning changes the ability of people to fully control the communication devices that are intrinsically connected to all facets of their lives and to limit what information those devices share.[58] Moreover, in

[52] See A/HRC/29/32.
[53] Ibid., para. 39.
[54] A/HRC/39/29, para. 20.
[55] A/HRC/29/32, para. 41.
[56] See https://cdt.org/wp-content/uploads/2021/08/CDT-Coalition-ltr-to-Apple-19-August-2021.pdf.
[57] 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); see also draft Online Safety Bill in the United Kingdom of Great Britain and Northern Ireland, available at https://www.gov.uk/government/publications/draft-online-safety-bill.
[58] Submissions by the Global Encryption Coalition Steering Committee and Privacy International.

the general scanning of communications, frequent false positives cannot be avoided, even if accuracy rates are high, thereby implicating numerous innocent individuals.[59] 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.[60]

28. Client-side scanning also opens up new security challenges, making security breaches more likely.[61] The screening process can also be manipulated, making it possible to artificially create false positive or false negative profiles.[62] Even if, for current purposes, client-side screening is narrowly tailored, opening up devices for Government-mandated screening is likely to lead to future attempts to widen the scope of content that is the target of such measures.[63] In particular, where the rule of law is weak and human rights are under threat, the impact of client-side screening could be much broader, for example it could be used to suppress political debate or to target opposition figures, journalists and human rights defenders.[64] Given the broad range of significant risks to human rights protection from mandated general client-side screening, such requirements should not be imposed without further substantial consideration of their potential human rights impacts and measures that mitigate those harms. Without in-depth investigation and analysis, it seems unlikely that such restrictions could be considered proportionate under international human rights law, even when imposed in pursuit of legitimate aims, given the severity of their possible consequences.[65]

III. Surveillance of the public

29. The High Commissioner has raised concerns about mass surveillance on several occasions, in particular in terms of the bulk interception of communications.[66] While some States have improved safeguards against surveillance, the deeply troubling practice of surveilling the online activities of large proportions of the population, or even entire populations, has not ceased. While previous reports have focused mostly on surveillance of private communications, they have touched less upon the privacy implications of the monitoring of public places, which is discussed below.

A. Surveillance of public places

30. Surveillance cameras, deployed to monitor public streets, car parks, transportation hubs and other public places, have become common in many countries. The number of

[59] See https://doi.org/10.48550/arXiv.2110.07450.

[60] For more information on the chilling effects of surveillance, see para. 47 below.

[61] Compared to attacks on corporate servers, attacks on personal devices can be executed by more actors and on less-secure infrastructure. Adversaries can use their access to the device to reverse engineer the scanning mechanism, see https://doi.org/10.48550/arXiv.2110.07450.

[62] https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha; and https://openreview.net/forum?id=CQbqeGAM_Ki.

[63] https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/; https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha; and https://doi.org/10.48550/arXiv.2110.07450.

[64] Ibid.

[65] A/HRC/39/29, para. 20, and A/HRC/29/32, para. 43. The views of the Court of Justice of the European Union lend support to this conclusion. The court recently ruled that the automated analysis of traffic and location data in a general and indiscriminate way must be limited to what is strictly necessary to respond to a serious, genuine, present or foreseeable threat to national security. The court rejected any other justification. See *La Quadrature du Net and Others v. Premier ministre and Others*, judgment of 6 October 2020 (joined cases C-511/18, C-512/18 and C-520/18), para. 177. Moreover, its case law indicates even stronger scepticism towards screening of content data, Court of Justice of the European Union, *Maximillan Schrems v. Data Protection Commissioner*, judgment of 6 October 2015 (C-362/14), para. 94.

[66] See A/HRC/27/37; A/HRC/39/29; and https://www.ohchr.org/en/press-releases/2013/07/mass-surveillance-pillay-urges-respect-right-privacy-and-protection.

surveillance cameras in use globally was expected to exceed one billion in 2021.[67] The 10 cities in the world with the highest video surveillance density operate between around 39 to over 115 surveillance cameras per 1,000 inhabitants.[68]

31. In addition to State-operated surveillance systems, some companies have integrated surveillance tools for private use, with dedicated features to report incidents to the authorities or even grant them direct access to their data streams.[69] This vastly expands the public space under surveillance, while undercutting transparency, oversight and accountability.

32. In recent years, the capabilities of surveillance cameras have dramatically increased as a result of the addition of sophisticated video analytics capacities. It is estimated that in 2010 less than 2 per cent of network cameras sold featured embedded video analytics, but this proportion had grown to over 40 per cent by 2016 and is likely to continue to grow.[70] Analytics features increasingly rely on artificial intelligence. Added capacities to carry out facial recognition and identify behaviour as suspicious are among the most problematic features of sophisticated video surveillance systems.[71] In addition, the use of drones for surveillances purposes has been normalized in many countries, where they are used for monitoring protests and other assemblies.[72]

33. Under the umbrella term "smart cities", a growing number of data-driven initiatives are under way to reshape urban spaces. Smart cities projects focus on the collection and processing of data to inform the management of city facilities, enabled by ever more capable sensor technologies. While much of the data collected and processed in these contexts relate to issues such as data on traffic flows, pollution or noise apart from the realm of personal data, other data collected can be easily linked to individuals, such as license plates and smart meter data. Moreover, seemingly anonymous data can often be de-anonymized,[73] and infrastructure, such as cameras installed for monitoring traffic data flows, can be repurposed for tracking individuals.[74]

34. These developments often occur against a background of new identity systems and expanded biometric databases. Across a range of countries, identity systems are linked to extensive central storage of personal data, including biometric information such as fingerprints, facial geometry, iris scans and DNA. Moreover, databases are often interlinked and made available for searching by other agencies. As a consequence, identifying individuals wherever they are located has become easier and easier.

B. Online monitoring

35. In parallel, monitoring of public online discourse has become widespread. Globally, many authorities are collecting and analysing social media posts and the private and professional networks built on publicly accessible communications platforms. Such social media intelligence ranges from the investigation of specific users to dragnet collection, storage and analysis of vast amounts of data. The data obtained may include: names; ages; photos and related digital templates; addresses; posts and reactions to other people's posts; social and professional contacts and associated networks; location data; interests; sexual orientation; gender identification; political affiliation and activities; religious beliefs; and health information.

[67] See https://venturebeat.com/2022/06/18/how-ml-powered-video-surveillance-could-improve-security/.

[68] See https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/; and https://surfshark.com/surveillance-cities.

[69] See https://www.accessnow.org/amazon-ring-privacy-review/.

[70] See https://cdn.ihs.com/www/pdf/IHS-Markit-Technology-Video-surveillance.pdf.

[71] See submissions by Derechos Digitales and the International Network of Civil Liberties Organizations.

[72] See submissions by Amnesty International and CIVICUS.

[73] See https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf.

[74] For more on the human rights impacts of smart cities, see https://www.amnesty.org/en/latest/research/2019/06/smart-cities-dreams-capable-of-becoming-nightmares/; and https://carrcenter.hks.harvard.edu/files/cchr/files/CCDP_006.pdf.

36. Oftentimes, various types of predictive analytics form part of social media intelligence practices, including attempts to identify possible crime hotspots. However, such analytics can also be used to assess the past, present and future behaviour of individuals and to assign risk scores relating to the likelihood that they may become offenders or security threats.[75] Social media intelligence is also used to predict the possibility of social unrest.[76]

37. These activities can serve manifold legitimate and illegitimate objectives, from crime investigation and prevention to vetting applicants for social benefits, monitoring protests, measuring public sentiment and profiling people's social conduct.[77]

C. Human rights impacts

38. Modern data-driven technologies are dramatically shifting the balance of power between the entity carrying out the surveillance and those being monitored. Before the advent of large-scale automated surveillance and data analytics tools, there were practical limitations to surveillance that provided a certain level of protection for individuals, even when in public.[78] Sophisticated digital tools render those past "natural" protections moot. Today, a single officer can monitor the social media accounts of dozens of people and, with the assistance of advanced software and big data analytics, small teams can observe and profile thousands of accounts.[79]

39. Similar developments enhance the efficacy and reach of other surveillance measures of public spaces. For example, the rise of facial recognition technology alongside other biometric recognition technologies has fundamentally transformed traditional practices of audiovisual monitoring as it has dramatically increased the capacity to identify individuals in public spaces, including participants in assemblies. Live facial recognition technology permits real-time identification of individuals, as well as their targeted surveillance and tracking. Retrospect identification of people may possibly further the range of data sources, leading to impacts that can be equally intrusive[80] if not deployed with utmost restraint.

40. The impact of public surveillance on human rights is further aggravated because data sources are increasingly merged, for example by combining facial recognition-equipped video surveillance feeds with social media data[81] and government databases, including information on social security, migration, terrorism suspects, arrests or even lists of individuals flagged for political reasons.

41. In addition, States rely on vast data collections amassed by a variety of private companies. In previous reports, the High Commissioner and special rapporteurs have highlighted the issue of Governments requesting access to data collected by telecommunications and Internet service providers, often against the background of mandatory data retention laws.[82] The range of companies receiving such requests is growing steadily. Some States compel companies to give them direct access to the data streams running through their networks. Such systems of direct access are of serious concern, as they are particularly prone to abuse and tend to circumvent key procedural safeguards.[83]

42. Moreover, States increasingly rely on surveillance services offered by business enterprises, for example by acquiring data from data brokers and other companies collecting and selling personal data.[84] Such practices can circumvent crucial procedural restrictions and

[75] See https://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2/, p. 152.
[76] See https://dx.doi.org/10.2139/ssrn.2702426, p. 1.
[77] See https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.
[78] A/HRC/44/24, para. 34.
[79] See https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.
[80] See submission by Amnesty International.
[81] See submission by the International Network of Civil Liberties Organizations.
[82] A/HRC/27/37, para. 26; A/HRC/39/29, para. 18; A/HRC/23/40 and A/HRC/23/40/Corr.1, paras. 65–67; and A/69/397, paras. 53–55.
[83] A/HRC/39/29, para. 19.
[84] See, for example, https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances; and https://www.accessnow.org/cms/assets/uploads/2020/07/Defending-Peaceful-Assembly-Association-Digital-Age.pdf, p. 25.

safeguards, allowing States to indirectly access tools that they could not have deployed themselves without contravening their human rights obligations. For example, the facial recognition tool developed by the company Clearview AI has been used by thousands of law enforcement agencies, despite the fact that it had been built by scraping the photos of billions of people from the Internet, a massive intrusion of privacy rights.[85]

43. Systematic surveillance of people in the public space online and offline, in particular when combined with additional ways to analyse and connect the obtained information with other data sources, constitutes an interference with the right to privacy and can have highly detrimental effects on the enjoyment of other human rights.[86] It may constitute a threat to freedom of expression and peaceful assembly, participation and democracy and should therefore be approached with utmost caution and only in strict adherence with human rights requirements. This is the case even though the activities monitored are occurring in public, or on open social media platforms, as individuals should have a space free from systematic observation and intrusion, in particular by government entities. As previously noted by the High Commissioner, the protection of the right to privacy extends to public spaces and information that is publicly available.[87] The Human Rights Committee has rejected the notion that data gathered in public areas is automatically in the public domain and may be freely accessed.[88] The European Court of Human Rights has recognized that publicly available or perceptible information may well fall within the scope of the right to privacy, in particular when personal data are systematically or permanently recorded.[89]

44. One particular concern in public surveillance relates to the recording of photographic images. People's images embody key attributes of their personality and reveal unique characteristics distinguishing them from other persons. Recording, analysing and retaining facial images of individuals without their consent constitute interference with their right to privacy. By deploying facial recognition technology in public spaces, which requires the collection and processing of facial images of all persons captured on camera, such interference is occurring on a mass and indiscriminate scale.[90]

45. Moreover, public surveillance measures can lead to, and often are, the basis of measures that directly affect individuals and communities, including coercive measures. Such measures include increased monitoring and policing of certain neighbourhoods, groups or individuals, sometimes leading to the interrogation, arrest and detention of individuals. Some groups and individuals may also be flagged as potential threats or risks, for example as potential terrorists or criminals, often without a robust basis in fact. Several Governments use the results of a variety of public surveillance measures to identify their critics or people not conforming to social expectations, which can lead to harassment, detention or the denial of essential services.[91]

---

[85] Various data protection authorities, determining that Clearview AI had violated data protection law, imposed heavy fines and/or ordered the erasure of personal data obtained, see https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/; see also https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy; https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en; and https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-met-en-demeure-clearview-ai-de-cesser-la-reutilisation-de. Data protection authorities have held that police forces, by using the tool, had violated data protection law, see https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en; and https://edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_en.

[86] See CCPR/C/NGA/CO/2, in which the Human Rights Committee expressed concern about social media monitoring, para. 40.

[87] A/HRC/39/29, para. 6.

[88] CCPR/C/COL/CO/7, para. 32.

[89] See European Court of Human Rights, *Rotaru v. Romania*, para. 43, judgment of 4 May 2000; *Peck v. the United Kingdom*, judgment of 28 January 2003, para. 59; *Perry v. the United Kingdom*, judgment of 17 July 2003, para. 38; and *Vukota-Bojić v. Switzerland*, judgment of 18 January 2017, para. 55.

[90] A/HRC/44/24, para. 33.

[91] See https://privacyinternational.org/explainer/55/social-media-intelligence.

46. Surveillance operations tend to disproportionately target minorities and marginalized communities.[92] The use of artificial intelligence risks perpetuating such patterns of discrimination,[93] including the use of facial recognition technologies for racial and ethnic profiling.[94] Predictive systems for policing and the administration of justice have been shown to disproportionately affect minorities.[95]

47. In addition, surveillance has considerable chilling effects on how people exercise their rights, in particular the rights to freedom of expression and peaceful assembly.[96] Various studies illustrate the extent of such effects. A 2015 survey revealed that 25 per cent of participants who were aware of the case of Edward Snowden had changed their use of various technology platforms.[97] Another study found that between 34 per cent to 61 per cent of writers (depending on the country concerned) had avoided or at least considered avoiding certain topics in their work owing to fear of government surveillance.[98] In a survey conducted by the Norwegian Board of Technology, 39 per cent of respondents stated that they would avoid using words and phrases that are monitored by the police.[99] As previously pointed out by the High Commissioner, such chilling effects extend to assemblies, including peaceful protests.[100]

D. Human rights requirements

48. Public surveillance undoubtedly entails substantial human rights risks and can substantially undermine the right to privacy. It is thus essential that States resorting to the use of public surveillance assess the potential human rights impacts of their actions and strictly ensure compliance with international human rights law, which requires that any such interference or restriction be based in law, necessary to achieve a legitimate aim and proportional. Current public surveillance measures often fail to meet those requirements.

49. Legality: despite the far-reaching impacts of the various forms of public surveillance, adequate applicable legal frameworks are largely missing in many countries. Data protection laws are often missing, inadequate or make broad exceptions for law enforcement and intelligence services.[101] Moreover, oftentimes, general data privacy laws do not provide detailed guidance or ensure adequate limitations on the use of specific surveillance tools. In

[92] See CERD/C/CHN/CO/14-17; and https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media.

[93] See the conference room paper of the High Commissioner on the promotion and protection of the human rights and fundamental freedoms of Africans and of people of African descent against excessive use of force and other human rights violations by law enforcement officers, paras. 93 and 94. Available from https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session47/list-reports.

[94] A/HRC/41/35, para. 12, and A/HRC/44/57, para. 39.

[95] Committee on the Elimination of Racial Discrimination, general recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials, paras. 33–34; A/HRC/44/57, para. 43; conference room paper of the High Commissioner on the promotion and protection of the human rights and fundamental freedoms of Africans and of people of African descent against excessive use of force and other human rights violations by law enforcement officers, para. 93; A/HRC/48/31, para. 24; https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/; https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf; and https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

[96] A/HRC/27/37, para. 20; see, with regard to protests: A/HRC/44/24, paras. 29, 35 and 52; European Court of Human Rights, *Big Brother Watch and Others v. the United Kingdom*, judgment of 25 May 2021 (58170/13, 62322/14 and 24960/15), para. 495; http://dx.doi.org/10.15779/Z38SS13; https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf; and https://pen.org/research-resources/global-chilling/.

[97] See https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf.

[98] See https://pen.org/research-resources/global-chilling/.

[99] See https://teknologiradet.no/wp-content/uploads/sites/105/2018/05/Online-with-the-public.pdf.

[100] A/HRC/44/24, paras. 35 and 53.

[101] A/HRC/39/29, para. 34.

this regard, dedicated legal instruments are required, in particular for surveillance done in the context of law enforcement and national security.[102] Laws and regulations need to have clearly determined and strict limitations on the access and merging of government databases. Unfortunately, there are few signs that States are moving towards regulating the use of social media intelligence techniques, technologies and tools. While there are increasing efforts by regulators and lawmakers at the local, national and regional level to regulate facial recognition and other biometric surveillance tools,[103] most authorities are continuing to operate biometric surveillance systems despite the lack of a legal basis for such activity.

50. Legitimate goals: there is no doubt that public surveillance can serve a broad range of legitimate goals, for example the protection of people's lives or bodily integrity and the security of critical infrastructure. Regrettably, public surveillance is routinely conducted for aims that are not permissible under international human rights law. Public surveillance has been unduly used, inter alia, to identify and track political dissenters, to carry out racial and ethnic profiling, to target communities of lesbian, gay, bisexual, transgender and intersex persons and to assess people's conformity with social norms.

51. Necessity and proportionality: while public surveillance may be permissible, States must demonstrate that measures are both necessary and proportionate. However, the effectiveness of surveillance measures is often doubtful, raising serious questions as to their necessity or proportionality. Evidence on the effect of video surveillance on safety and crime prevention is mixed. Most studies point to, at most, modest reductions in some types of crime (such as vehicle and property related crime) in areas monitored by surveillance cameras, while, in general, violent crime does not seem to be affected by the presence of surveillance cameras.[104] Moreover, a comparison between numerous municipalities in various jurisdictions shows little to no correlation between the number of public surveillance cameras and crime or safety across an entire municipality.[105] With regard to automated threat detection, a system widely used by police forces for detecting gunshots to identify possible crime scenes, it has been shown to wrongly identify sounds as gunshots in 89 per cent of cases.[106] Finally, many police departments that signed up for predictive policing services have since ended these collaborations, citing limited usefulness.[107]

52. General monitoring of people in public spaces is almost invariably disproportionate. Surveillance measures in public spaces should be targeted and should address a concrete legitimate aim, such as averting a specific threat to public safety or security that is significant enough to outweigh their adverse human rights impacts. Such measures need to be limited, focused on specific locations and times, for instance, when evidence indicates that a crime is likely to occur or that threats to public safety and security may emerge. No less privacy-invasive alternative should be available. It is essential to impose strict limitations on the duration of storage of captured data and the associated purposes for which such data is to be used. Remote biometric surveillance systems, in particular, raise serious concerns with regard to their proportionality, given their highly intrusive nature and broad impact on large numbers of people.[108] Against this background, the High Commissioner has welcomed recent efforts

[102] Minimum requirements for surveillance laws have previously been outlined by the High Commissioner, see A/HRC/27/37 and A/HRC/39/29.

[103] See the proposed European Union Artificial Intelligence Act; the European Data Protection Board Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 1.0, available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en; see also law in Washington State, United States of America, relating to the use of facial recognition, available at https://www.securityindustry.org/report/washington-facial-recognition-law-faq/; and bans and moratoriums adopted by local and regional legislatures.

[104] See https://academicworks.cuny.edu/jj_pubs/256/; and https://doi.org/10.1080/01924036.2021.1879885.

[105] See https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

[106] See https://www.macarthurjustice.org/blog/shotspotter-is-a-failure-whats-next/; and https://igchicago.org/2021/08/24/oig-finds-that-shotspotter-alerts-rarely-lead-to-evidence-of-a-gun-related-crime-and-that-presence-of-the-technology-changes-police-behavior/.

[107] See https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

[108] A/HRC/48/31, paras. 26–27; and A/HRC/44/24, paras. 33–38.

to limit or ban the use of remote biometric recognition technologies and has called for a moratorium on its use in public spaces, at least until key safeguards are in place.[109] If used at all, such technologies should only be deployed to respond to situations such as serious crime and serious public safety threats, if discriminatory effects can be excluded and subjected to adequate and effective oversight, including independent authorization and regular independent human rights audits.

IV. Conclusions and recommendations

53. **The present report provides a snapshot of several key areas in which the right to privacy in the digital realm is currently being threatened. The rapid adoption of digital technologies raises a range of additional challenges that are not covered in this report but would be worthy of further attention. For example, covert mass surveillance, discussed in previous reports of the High Commissioner,[110] remains a serious problem. Equally, the human rights implications of digital identity systems and the various use cases of biometrics are little understood, despite their worldwide roll-out. Pervasive tracking of Internet users by countless companies, such as advertisers, financial institutions and data brokers, require far more attention in international human rights forums. The coronavirus disease (COVID-19) pandemic and the dizzying array of digital responses to it could be the subject of a report unto itself. The ways privacy violations and abuses affect marginalized people and people in vulnerable position must be more deeply explored and understood. Emerging phenomena, such as the push for widespread adoption of blockchain, expanded and virtual reality technologies and the development of increasingly powerful neurotechnology, should be followed very closely.**

54. **However, even while focusing on only a few key developments, the present report depicts a troubling picture of how the right to privacy is being steadily undermined in the digital age. This analysis should not be understood as denying the enormous benefits digital technologies are bringing to societies – on the contrary, societies should fully embrace technological progress that empowers people, improves lives, strengthens justice and boosts productivity. But the manifold ways in which pervasive surveillance threatens human rights and the rule of law and may erode vibrant, pluralistic democracies are profoundly alarming. The features of modern networked digital technologies can make them formidable tools for control and oppression: each action in the digital space leaves a data trail; cloud computing technology facilitates the fusion and analysis of disparate data sources; automation boosts the possible scope and efficacy of surveillance; and digital surveillance is difficult to observe by those subjected to it. Moreover, digital surveillance is intimately linked to a lack of transparency more generally. The public often knows very little about the various surveillance practices being interwoven throughout many aspects of life. Governments too often fail to release reliable information on what kind of surveillance systems they use and for what purposes – and often neglect to present evidence on the efficacy of those systems.**

55. **Measures of surveillance that are incompatible with international human rights law are already widespread. Even where surveillance serves legitimate purposes, the underlying infrastructure can easily be repurposed, oftentimes serving ends for which it was not originally intended (so-called "function creep") or following changes in the political landscape. Decision makers should keep this in mind when considering new projects that enhance powers to collect and analyse personal data. Public debates about the boundaries of surveillance are urgently needed. Without an active public discussion, societies risk sleepwalking into surveillance systems allowing those in power to exert unprecedented levels of control over day-to-day life.**

56. **With this in mind, OHCHR recommends that States:**

(a) **Ensure that any interference with the right to privacy, including hacking, restrictions to access and use of encryption technology and surveillance of the public,**

[109] A/HRC/48/31, paras. 27 and 59 (d).
[110] See A/HRC/27/37 and A/HRC/39/29.

complies with international human rights law, including the principles of legality, legitimate aim, necessity and proportionality and non-discrimination, and does not impair the essence of that right;

(b) **Conduct human rights due diligence systematically, including regular comprehensive human rights impact assessments, when designing, developing, purchasing, deploying and operating surveillance systems;**

(c) **Take into account, when conducting human rights due diligence and assessing the necessity and proportionality of new surveillance systems and powers, the entire legal and technological environment in which those systems or powers are or would be embedded; States should also consider risks of abuse, function creep and repurposing, including risks as a result of future political changes;**

(d) **Adopt and effectively enforce, through independent, impartial and well-resourced authorities, data privacy legislation for the public and private sectors that complies with international human rights law, including safeguards, oversight and remedies to effectively protect the right to privacy;**

(e) **Take immediate measures to effectively increase the transparency of the use of surveillance technologies, including by appropriately informing the public and affected individuals and communities and regularly providing data relevant for the public to assess their efficacy and impact on human rights;**

(f) **Promote public debate of the use of surveillance technologies and ensure meaningful participation of all stakeholders in decisions on the acquisition, transfer, sale, development, deployment and use of surveillance technologies, including the elaboration of public policies and their implementation;**

(g) **Implement moratoriums on the domestic and transnational sale and use of surveillance systems, such as hacking tools and biometric systems that can be used for the identification or classification of individuals in public places, until adequate safeguards to protect human rights are in place; such safeguards should include domestic and export control measures, in line with the recommendations made herein and in previous reports to the Human Rights Council;**[111]

(h) **Ensure that victims of human rights violations and abuses linked to the use of surveillance systems have access to effective remedies.**

57. **In relation to the specific issues raised in the present report, OHCHR recommends that States:**

Hacking

(a) **Ensure that the hacking of personal devices is employed by authorities only as a last resort, used only to prevent or investigate a specific act amounting to a serious threat to national security or a specific serious crime, and narrowly targeted at the person suspected of committing those acts; such measures should be subject to strict independent oversight and should require prior approval by a judicial body;**

Encryption

(b) **Promote and protect strong encryption and avoid all direct, or indirect, general and indiscriminate restrictions on the use of encryption, such as prohibitions, criminalization, the imposition of weak encryption standards or requirements for mandatory general client-side scanning; interference with the encryption of private communications of individuals should only be carried out when authorized by an independent judiciary body and on a case-by-case basis, targeting individuals if strictly necessary for the investigation of serious crimes or the prevention of serious crimes or serious threats to public safety or national security;**

[111] See A/HRC/27/37, A/HRC/39/29, A/HRC/44/24, and A/HRC/48/31.

Surveillance of public spaces and export control of surveillance technology

(c) **Adopt adequate legal frameworks to govern the collection, analysis and sharing of social media intelligence that clearly define permissible grounds, prerequisites, authorization procedures and adequate oversight mechanisms;**

(d) **Avoid general privacy-intrusive monitoring of public spaces and ensure that all public surveillance measures are strictly necessary and proportionate for achieving important legitimate objectives, including by strictly limiting their location and time, as well as the duration of data storage, the purpose of data use and access to data; biometric recognition systems should only be used in public spaces to prevent or investigate serious crimes or serious public safety threats and if all requirements under international human rights law are implemented with regard to public spaces;**[112]

(e) **Establish robust well-tailored export control regimes applicable to surveillance technologies, the use of which carries high risks for the enjoyment of human rights; States should require transparent human rights impact assessments that take into account the capacities of the technologies at issue as well as the situation in the recipient State, including compliance with human rights, adherence to the rule of law, the existence and effective enforcement of applicable laws regulating surveillance activities and the existence of independent oversight mechanisms;**

(f) **Ensure that, in the provision and use of surveillance technologies, public-private partnerships uphold and expressly incorporate human rights standards and do not result in an abdication of governmental accountability for human rights.**

[112] Including the requirements set out in A/HRC/44/24, para. 53 (j) (i–v), and A/HRC/48/31, para. 59 (d).