United Nations A/HRC/27/37*

General Assembly

Distr.: General
30 June 2014

Original: English

Human Rights Council
Twenty-seventh session
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

In its resolution 68/167, the General Assembly requested the United Nations High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session, with views and recommendations, to be considered by Member States. The present report is submitted pursuant to that request. The Office of the High Commissioner will also submit the report to the General Assembly at its sixty-ninth session, pursuant to the request of the Assembly.

* Reissued for technical reasons on 18 July 2014.

GE.14-08854 (E)
1408854

Contents

I. Introduction

1. Digital communications technologies, such as the Internet, mobile smartphones and WiFi-enabled devices, have become part of everyday life. By dramatically improving access to information and real-time communication, innovations in communications technology have boosted freedom of expression, facilitated global debate and fostered democratic participation. By amplifying the voices of human rights defenders and providing them with new tools to document and expose abuses, these powerful technologies offer the promise of improved enjoyment of human rights. As contemporary life is played out ever more online, the Internet has become both ubiquitous and increasingly intimate.

2. In the digital era, communications technologies also have enhanced the capacity of Governments, enterprises and individuals to conduct surveillance, interception and data collection. As noted by the Special Rapporteur on the right to freedom of expression and opinion, technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. The State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before.[1] In other words, the technological platforms upon which global political, economic and social life are increasingly reliant are not only vulnerable to mass surveillance, they may actually facilitate it.

3. Deep concerns have been expressed as policies and practices that exploit the vulnerability of digital communications technologies to electronic surveillance and interception in countries across the globe have been exposed. Examples of overt and covert digital surveillance in jurisdictions around the world have proliferated, with governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure. Governments reportedly have threatened to ban the services of telecommunication and wireless equipment companies unless given direct access to communication traffic, tapped fibre-optic cables for surveillance purposes, and required companies systematically to disclose bulk information on customers and employees. Furthermore, some have reportedly made use of surveillance of telecommunications networks to target political opposition members and/or political dissidents. There are reports that authorities in some States routinely record all phone calls and retain them for analysis, while the monitoring by host Governments of communications at global events has been reported. Authorities in one State reportedly require all personal computers sold in the country to be equipped with filtering software that may have other surveillance capabilities. Even non-State groups are now reportedly developing sophisticated digital surveillance capabilities. Mass surveillance technologies are now entering the global market, raising the risk that digital surveillance will escape governmental controls.

4. Concerns have been amplified following revelations in 2013 and 2014 that suggested that, together, the National Security Agency in the United States of America and General Communications Headquarters in the United Kingdom of Great Britain and Northern Ireland have developed technologies allowing access to much global internet traffic, calling records in the United States, individuals' electronic address books and huge volumes of other digital communications content. These technologies have reportedly been deployed through a transnational network comprising strategic intelligence relationships between Governments, regulatory control of private companies and commercial contracts.

[1] A/HRC/23/40, para. 33.

5. Following on the concerns of Member States and other stakeholders at the negative impact of these surveillance practices on human rights, in December 2013 the General Assembly adopted resolution 68/167, without a vote, on the right to privacy in the digital age. In the resolution, which was co-sponsored by 57 Member States, the Assembly affirmed that the rights held by people offline must also be protected online, and called upon all States to respect and protect the right to privacy in digital communication. It further called upon all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data, emphasizing the need for States to ensure the full and effective implementation of their obligations under international human rights law.

6. Also in resolution 68/167, the General Assembly requested the United Nations High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session, with views and recommendations, to be considered by Member States. The present report is submitted pursuant to that request. As mandated by resolution 68/167, the Office of the High Commissioner (OHCHR) will also submit the report to the Assembly at its sixty-ninth session.

II. Background and methodology

7. Bearing in mind resolution 68/167, OHCHR participated in a number of events and gathered information from a broad range of sources. On 24 February 2014, the High Commissioner delivered a keynote presentation at an expert seminar on "The right to privacy in the digital age", which was co-sponsored by Austria, Brazil, Germany, Liechtenstein, Mexico, Norway and Switzerland, and facilitated by the Geneva Academy on International Humanitarian Law and Human Rights.

8. From November 2013 to March 2014, OHCHR engaged the United Nations University in a research project on the application of international human rights law to national regimes overseeing governmental digital surveillance. OHCHR is grateful to the University, and acknowledges its major substantive contribution to the preparation of the present report through the research project.

9. As part of an open consultation, on 27 February 2014, OHCHR addressed a questionnaire to Member States through their Permanent Missions in Geneva and in New York; international and regional organizations; national human rights institutions; non-governmental organizations; and business entities. In its questionnaire, OHCHR invited inputs on the issues as addressed by the General Assembly in its resolution 68/167. A dedicated OHCHR webpage was created in order to make available the questionnaire and all contributions for public consultation, as well as to provide further opportunity for input. Contributions were received from 29 Member States from all regions, five international and/or regional organizations, three national human rights institutions, 16 non-governmental organizations and two private sector initiatives.[2]

10. Many of the contributions referred in detail to existing national legislative frameworks and to other measures taken to ensure respect for and protection of the right to privacy in the digital age, as well as to initiatives to establish and implement procedural safeguards and effective oversight. Some contributions referred to challenges encountered

[2] All contributions are available at www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

in the implementation of the right to privacy in the digital age, and provided suggestions for initiatives at the international level. They included encouragement to the Human Rights Committee to update its relevant general comments, in particular on article 17 of the International Covenant on Civil and Political Rights; the establishment by the Human Rights Council of a special procedures mandate on the right to privacy; and/or the engagement of existing relevant special procedures mandate holders in joint or individual initiatives to address issues related to the right to privacy in the context of digital surveillance and to provide good-practice guidance.

11. Pursuant to the request made in General Assembly resolution 68/167, the present report offers reflections and recommendations based on an assessment of information available at the time of drafting, drawing also on the wealth of material reflected in the diverse range of contributions received.

III. Issues relating to the right to privacy in the digital age

12. As recalled by the General Assembly in its resolution 68/167, international human rights law provides the universal framework against which any interference in individual privacy rights must be assessed. Article 12 of the Universal Declaration of Human Rights provides that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." The International Covenant on Civil and Political Rights, to date ratified by 167 States, provides in article 17 that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation". It further states that "everyone has the right to the protection of the law against such interference or attacks."

13. Other international human rights instruments contain similar provisions. Laws at the regional and national levels also reflect the right of all people to respect for their private and family life, home and correspondence or the right to recognition and respect for their dignity, personal integrity or reputation. In other words, there is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice.

14. While the mandate for the present report focused on the right to privacy, it should be underscored that other rights also may be affected by mass surveillance, the interception of digital communications and the collection of personal data. These include the rights to freedom of opinion and expression, and to seek, receive and impart information; to freedom of peaceful assembly and association; and to family life – rights all linked closely with the right to privacy and, increasingly, exercised through digital media. Other rights, such as the right to health, may also be affected by digital surveillance practices, for example where an individual refrains from seeking or communicating sensitive health-related information for fear that his or her anonymity may be compromised. There are credible indications to suggest that digital technologies have been used to gather information that has then led to torture and other ill-treatment. Reports also indicate that metadata derived from electronic surveillance have been analysed to identify the location of targets for lethal drone strikes. Such strikes continue to raise grave concerns over compliance with international human rights law and humanitarian law, and accountability for any violations thereof. The linkages between mass surveillance and these other effects on human rights, while beyond the scope of the present report, merit further consideration.

A. The right to protection against arbitrary or unlawful interference with privacy, family, home or correspondence

15. Several contributions highlighted that, when conducted in compliance with the law, including international human rights law, surveillance of electronic communications data can be a necessary and effective measure for legitimate law enforcement or intelligence purposes. Revelations about digital mass surveillance have, however, raised questions around the extent to which such measures are consistent with international legal standards and whether stronger surveillance safeguards are needed to protect against violations of human rights. Specifically, surveillance measures must not arbitrarily or unlawfully interfere with an individual's privacy, family, home or correspondence; Governments must take specific measures to ensure protection of the law against such interference.

16. A review of the various contributions received revealed that addressing these questions requires an assessment of what constitutes interference with privacy in the context of digital communications; of the meaning of "arbitrary and unlawful"; and of whose rights are protected under international human rights law, and where. The sections below address issues that were highlighted in various contributions.

1. Interference with privacy

17. International and regional human rights treaty bodies, courts, commissions and independent experts have all provided relevant guidance with regard to the scope and content of the right to privacy, including the meaning of "interference" with an individual's privacy. In its general comment No. 16, the Human Rights Committee underlined that compliance with article 17 of the International Covenant on Civil and Political Rights required that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. "Correspondence should be delivered to the addressee without interception and without being opened or otherwise read".[3]

18. It has been suggested by some that the conveyance and exchange of personal information via electronic means is part of a conscious compromise through which individuals voluntarily surrender information about themselves and their relationships in return for digital access to goods, services and information. Serious questions arise, however, about the extent to which consumers are truly aware of what data they are sharing, how and with whom, and to what use they will be put. According to one report, "a reality of big data is that once data is collected, it can be very difficult to keep anonymous. While there are promising research efforts underway to obscure personally identifiable information within large data sets, far more advanced efforts are presently in use to re-identify seemingly 'anonymous' data. Collective investment in the capability to fuse data is many times greater than investment in technologies that will enhance privacy." Furthermore, the authors of the report noted that "focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy", in part because "big data enables new, non-obvious, unexpectedly powerful uses of data".[4]

19. In a similar vein, it has been suggested that the interception or collection of data about a communication, as opposed to the content of the communication, does not on its

[3] *Official Records of the General Assembly, Forty-third Session, Supplement No. 40* (A/43/40), annex VI, para. 8.

[4] Executive Office of the President of the United States, "Big Data: Seizing Opportunities, Preserving Values", May 2014 (available from www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf), p. 54.

own constitute an interference with privacy. From the perspective of the right to privacy, this distinction is not persuasive. The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication. As the European Union Court of Justice recently observed, communications metadata "taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained."[5] Recognition of this evolution has prompted initiatives to reform existing policies and practices to ensure stronger protection of privacy.

20. It follows that any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy,[6] with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful.

2. What is "arbitrary" or "unlawful"?

21. Interference with an individual's right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful. In its general comment No. 16, the Human Rights Committee explained that the term "unlawful" implied that no interference could take place "except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant".[7] In other words, interference that is permissible under national law may nonetheless be "unlawful" if that national law is in conflict with the provisions of the International Covenant on Civil and Political Rights. The expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of this concept, the Committee explained, "is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances".[8] The Committee interpreted the concept of reasonableness to indicate that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case".[9]

22. Unlike certain other provisions of the Covenant, article 17 does not include an explicit limitations clause. Guidance on the meaning of the qualifying words "arbitrary or unlawful" nonetheless can be drawn from the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights;[10] the practice of the Human Rights Committee as reflected in its general comments, including

[5] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014, paras. 26-27, and 37. See also Executive Office of the President, "Big Data and Privacy: A Technological Perspective" (available from www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf), p. 19.

[6] See European Court of Human Rights, *Weber and Saravia v. Germany*, para. 78; *Malone v. UK*, para. 64.

[7] *Official Records of the General Assembly* (see footnote 3), para. 3.

[8] Ibid., para. 4.

[9] Communication No. 488/1992, *Toonan v. Australia*, para. 8.3; see also communications Nos. 903/1999, para 7.3, and 1482/2006, paras. 10.1 and 10.2.

[10] See E/CN.4/1985/4, annex.

Nos. 16, 27, 29, 34, and 31, findings on individual communications[11] and concluding observations;[12] regional and national case law;[13] and the views of independent experts.[14] In its general comment No. 31 on the nature of the general legal obligation on States parties to the Covenant, for example, the Human Rights Committee provides that States parties must refrain from violation of the rights recognized by the Covenant, and that "any restrictions on any of [those] rights must be permissible under the relevant provisions of the Covenant. Where such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights."[15] The Committee further underscored that "in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right."

23. These authoritative sources point to the overarching principles of legality, necessity and proportionality, the importance of which also was highlighted in many of the contributions received. To begin with, any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available.[16] Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.

24. Governments frequently justify digital communications surveillance programmes on the grounds of national security, including the risks posed by terrorism. Several contributions suggested that since digital communications technologies can be, and have been, used by individuals for criminal objectives (including recruitment for and the financing and commission of terrorist acts), the lawful, targeted surveillance of digital communication may constitute a necessary and effective measure for intelligence and/or law enforcement entities when conducted in compliance with international and domestic law. Surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a "legitimate aim" for purposes of an assessment from the viewpoint of article 17 of the Covenant. The degree of interference must, however, be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose.

25. In assessing the necessity of a measure, the Human Rights Committee, in its general comment No. 27, on article 12 of the International Covenant on Civil and Political Rights, stressed that that "the restrictions must not impair the essence of the right […]; the relation

[11] For example, communication No. 903/1999, 2004, *Van Hulst v. The Netherlands.*

[12] CCPR /C/USA/CO/4.

[13] For example, European Court of Human Rights, *Uzun v. Germany*, 2 September 2010, and *Weber and Soravia v. Germany*, para. 4; and Inter-American Court of Human Rights, *Escher v. Brazil*, Judgment, 20 November 2009.

[14] See A/HRC/13/37 and A/HRC/23/40. See also International Principles on the Application of Human Rights to Communications Surveillance, available from https://en.necessaryandproportionate.org/text.

[15] CCPR/C/21/Rev.1/Add. 13, para. 6.

[16] CCPR/C/21/Rev.1/Add.9, paras. 11 – 16. See also A/HRC/14/46, annex, practice 20.

between right and restriction, between norm and exception, must not be reversed."[17] The Committee further explained that "it is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them." Moreover, such measures must be proportionate: "the least intrusive instrument amongst those which might achieve the desired result".[18] Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.

26. Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of Governments on private sector actors to retain data "just in case" it is needed for government purposes. Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.[19]

27. One factor that must be considered in determining proportionality is what is done with bulk data and who may have access to them once collected. Many national frameworks lack "use limitations", instead allowing the collection of data for one legitimate aim, but subsequent use for others. The absence of effective use limitations has been exacerbated since 11 September 2001, with the line between criminal justice and protection of national security blurring significantly. The resulting sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating article 17 of the Covenant, because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another. A review of national practice in government access to third-party data found "when combined with the greater ease with which national security and law enforcement gain access to private-sector data in the first place, the expanding freedom to share that information among agencies and use it for purposes beyond those for which it was collected represents a substantial weakening of traditional data protections."[20] In several States, data-sharing regimes have been struck down by judicial review on such a basis. Others have suggested that such use limitations are a good practice to ensure the effective discharge of a State's obligations under article 17 of the Covenant,[21] with meaningful sanctions for their violation.

[17] CCPR/C/21/Rev.1/Add.9, paras. 11 – 16. See also European Court of Human Rights, *Handyside v. the United Kingdom*, para. 48; and *Klass v. Germany*, para. 42.

[18] CCPR/C/21/Rev.1/Add.9, paras. 11 – 16.

[19] See opinion of the Advocate-General Cruz Villalón of the Court of Justice of the European Union in joint cases C-293/12 and C-594/12, which suggests that the Directive 2006/24/EU (on the retention of data generated or processed in connection with the provision of electronic communications services) is "as a whole" in violation of the Charter of Fundamental Rights of the European Union because it fails to impose strict limits on such data retention. See also CCPR/C/USA/CO/4, para. 22.

[20] Fred H. Cate, James X. Dempsey and Ira S. Rubinstein, "Systematic government access to private-sector data", *International Data Privacy Law*, vol. 2, No. 4, 2012, p. 198.

[21] See A/HRC/14/46, annex, practice 23.

B. Protection of the law

28. Paragraph 2 of article 17 of the International Covenant on Civil and Political Rights explicitly states that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy. This implies that any communications surveillance programme must be conducted on the basis of a publicly accessible law, which in turn must comply with the State's own constitutional regime and international human rights law.[22] "Accessibility" requires not only that the law is published, but that it is sufficiently precise to enable the affected person to regulate his or her conduct, with foresight of the consequences that a given action may entail. The State must ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse. [23]

29. Consequently, secret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law".[24] Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion; the scope and manner of exercise of authoritative discretion granted must be indicated (in the law itself, or in binding, published guidelines) with reasonable clarity. A law that is accessible, but that does not have foreseeable effects, will not be adequate. The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight. Several States also require that the legal framework be established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive – a requirement that helps to ensure that the legal framework is not only accessible to the public concerned after its adoption, but also during its development, in accordance with article 25 of the International Covenant on Civil and Political Rights.[25]

30. The requirement of accessibility is also relevant when assessing the emerging practice of States to outsource surveillance tasks to others. There is credible information to suggest that some Governments systematically have routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. Reportedly, some Governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes. Such practice arguably fails the test of lawfulness because, as some contributions for the present report pointed out, it makes the operation of the surveillance regime unforeseeable for those affected by it. It may undermine the essence of the right protected by article 17 of the International Covenant on Civil and Political Rights, and would therefore be prohibited by article 5 thereof. States have also failed to take effective measures to protect individuals within their jurisdiction

[22] See ibid., annex.

[23] CCPR /C/USA/CO/4, para. 22. See also European Court of Human Rights, *Malone v. the United Kingdom*, No. 8691/79, 2 August 1984, paras. 67 and 68; and *Weber and Saravia v. Germany*, application no. 54934/00, 29 June 2006, in which the Court lists minimum safeguards that should be set out in statute law.

[24] See CCPR /C/USA/CO/4, para. 22.

[25] See also A/HRC/14/46.

against illegal surveillance practices by other States or business entities, in breach of their own human rights obligations.

C. Who is protected, and where?

31. The extraterritorial application of the International Covenant on Civil and Political Rights to digital surveillance was addressed in several of the contributions received. Whereas it is clear that certain aspects of the recently revealed surveillance programmes, for instance, will trigger the territorial obligations of States conducting surveillance, additional concerns have been expressed in relation to extraterritorial surveillance and the interception of communications.

32. Article 2 of the International Covenant on Civil and Political Rights requires each State party to respect and ensure to all persons within its territory and subject to its jurisdiction the rights recognized in the Covenant without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. The Human Rights Committee, in its general comment No. 31, affirmed that States parties are required by article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party."[26] This extends to persons within their "authority".[27]

33. The Human Rights Committee has been guided by the principle, as expressed even in its earliest jurisprudence, that a State may not avoid its international human rights obligations by taking action outside its territory that it would be prohibited from taking "at home".[28] This position is consonant with the views of the International Court of Justice, which has affirmed that the International Covenant on Civil and Political Rights is applicable in respect of acts done by a State "in the exercise of its jurisdiction outside its own territory",[29] as well as articles 31 and 32 of the Vienna Convention on the Law of Treaties. The notions of "power" and "effective control" are indicators of whether a State is exercising "jurisdiction" or governmental powers, the abuse of which human rights protections are intended to constrain. A State cannot avoid its human rights responsibilities simply by refraining from bringing those powers within the bounds of law. To conclude otherwise would not only undermine the universality and essence of the rights protected by international human rights law, but may also create structural incentives for States to outsource surveillance to each other.

34. It follows that digital surveillance therefore may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in

[26] CCPR/C/21/Rev.1/Add.13, para. 10.

[27] See *Official Records of the General Assembly, Thirty-sixth Session, Supplement No. 40* (A/36/40), annex XIX, para. 12.2; see also annex XX. See also CCPR/CO/78/ISR, para. 11; CCPR/CO/72/NET, para. 8; CCPR/CO/81/BEL, para. 6; and Inter-American Commission of Human Rights, *Coard et al. v. the United States*, case No. 10.951, Report No. 109/99, 29 September 1999, paras. 37, 39, 41 and 43.

[28] See *Official Records of the General Assembly, Thirty-sixth Session* (see footnote 27), annex XIX, paras. 12.2-12.3, and annex XX, para. 10.3.

[29] Advisory opinion of the International Court of Justice on the *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, of 9 July 2004 (A/ES-10/273 and Corr.1), paras. 107-111. See also International Court of Justice, case concerning *Armed Activities on the Territory of the Congo* (*Democratic Republic of the Congo v. Uganda*), judgment, 2005, p. 168.

relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protections must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violates another State's sovereignty.

35. This conclusion is equally important in the light of ongoing discussions on whether "foreigners" and "citizens" should have equal access to privacy protections within national security surveillance oversight regimes. Several legal regimes distinguish between the obligations owed to nationals or those within a State's territories, and non-nationals and those outside,[30] or otherwise provide foreign or external communications with lower levels of protection. If there is uncertainty around whether data are foreign or domestic, intelligence agencies will often treat the data as foreign (since digital communications regularly pass "off-shore" at some point) and thus allow them to be collected and retained. The result is significantly weaker – or even non-existent – privacy protection for foreigners and non-citizens, as compared with those of citizens.

36. International human rights law is explicit with regard to the principle of non-discrimination. Article 26 of the International Covenant on Civil and Political Rights provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law" and, further, that "in this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." These provisions are to be read together with articles 17, which provides that "no one shall be subjected to arbitrary interference with his privacy" and that "everyone has the right to the protection of the law against such interference or attacks", as well as with article 2, paragraph 1. In this regard, the Human Rights Committee has underscored the importance of "measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance."[31]

D. Procedural safeguards and effective oversight

37. Article 17, paragraph 2 of the International Covenant on Civil and Political Rights states that everyone has the right to the protection of the law against unlawful or arbitrary interference or attacks. The "protection of the law" must be given life through effective procedural safeguards, including effective, adequately resourced institutional arrangements. It is clear, however, that a lack of effective oversight has contributed to a lack of accountability for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Internal safeguards without independent, external monitoring in particular have proven ineffective against unlawful or arbitrary surveillance methods. While these safeguards may take a variety of forms, the involvement of all branches of government in

[30] See for example, in the United States, the Foreign Intelligence Surveillance Act S1881(a); in the United Kingdom, the Regulation of Investigatory Powers Act 2000, s8(4); in New Zealand, the Government Security Bureau Act 2003, s. 15A; in Australia, the Intelligence Services Act S. 9; and in Canada, the National Defence Act, S. 273.64 (1).

[31] CCPR /C/USA/CO/4, para. 22.

the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law.

38. Judicial involvement that meets international standards relating to independence, impartiality and transparency can help to make it more likely that the overall statutory regime will meet the minimum standards that international human rights law requires. At the same time, judicial involvement in oversight should not be viewed as a panacea; in several countries, judicial warranting or review of the digital surveillance activities of intelligence and/or law enforcement agencies have amounted effectively to an exercise in rubber-stamping. Attention is therefore turning increasingly towards mixed models of administrative, judicial and parliamentary oversight, a point highlighted in several contributions for the present report. There is particular interest in the creation of "public interest advocacy" positions within surveillance authorization processes. Given the growing role of third parties, such as Internet service providers, consideration may also need to be given to allowing such parties to participate in the authorization of surveillance measures affecting their interests or allowing them to challenge existing measures. The utility of independent advice, monitoring and/or review to help to ensure strict scrutiny of measures imposed under a statutory surveillance regime has been highlighted positively in relevant jurisprudence. Parliamentary committees also can play an important role; however, they may also lack the independence, resources or willingness to discover abuse, and may be subject to regulatory capture. Jurisprudence at the regional level has emphasized the utility of an entirely independent oversight body, particularly to monitor the execution of approved surveillance measures.[32] In 2009, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism suggested, therefore, that "there must be no secret surveillance system that is not under review of an independent oversight body and all interferences must be authorized through an independent body."[33]

E. Right to an effective remedy

39. The International Covenant on Civil and Political Rights requires States parties to ensure that victims of violations of the Covenant have an effective remedy. Article 2, paragraph 3 (b) further specifies that States parties to the Covenant undertake "to ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy". States must also ensure that the competent authorities enforce such remedies when granted. As the Human Rights Committee emphasized in its general comment No. 31, failure by a State party to investigate allegations of violations could in and of itself give rise to a separate breach of the Covenant.[34] Moreover, cessation of an ongoing violation is an essential element of the right to an effective remedy.

40. Effective remedies for violations of privacy through digital surveillance can thus come in a variety of judicial, legislative or administrative forms. Effective remedies typically share certain characteristics. First, those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated. Notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to

[32] See for example European Court of Human Rights, *Ekimdzhiev v. Bulgaria*, application No. 62540/00, 28 June 2007.

[33] A/HRC/13/37, para. 62.

[34] CCPR/C/21/Rev.1/Add. 13, para. 15.

challenge such measures) thus become critical issues in determining access to effective remedy. States take different approaches to notification: while some require post facto notification of surveillance targets, once investigations have concluded, many regimes do not provide for notification. Some may also formally require such notification in criminal cases; however, in practice, this stricture appears to be regularly ignored. There are also variable approaches at the national level to the issue of an individual's standing to bring a judicial challenge. The European Court of Human Rights ruled that, while the existence of a surveillance regime might interfere with privacy, a claim that this created a rights violation was justiciable only where there was a "reasonable likelihood" that a person had actually been subjected to unlawful surveillance.[35]

41. Second, effective remedies will involve prompt, thorough and impartial investigation of alleged violations. This may be provided through the provision of an "independent oversight body […] governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society."[36] Third, for remedies to be effective, they must be capable of ending ongoing violations, for example, through ordering deletion of data or other reparation.[37] Such remedial bodies must have "full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders".[38] Fourth, where human rights violations rise to the level of gross violations, non-judicial remedies will not be adequate, as criminal prosecution will be required.[39]

IV. What role for business?

42. There is strong evidence of a growing reliance by Governments on the private sector to conduct and facilitate digital surveillance. On every continent, Governments have used both formal legal mechanisms and covert methods to gain access to content, as well as to metadata. This process is increasingly formalized: as telecommunications service provision shifts from the public sector to the private sector, there has been a "delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of 'self-regulation' or 'cooperation'".[40] The enactment of statutory requirements for companies to make their networks "wiretap-ready" is a particular concern, not least because it creates an environment that facilitates sweeping surveillance measures.

[35] See *Esbester v. the United Kingdom*, application No. 18601/91, Commission decision of 2 April 1993; *Redgrave v. the United Kingdom*, application No. 202711/92, Commission decision of 1 September 1993; and *Matthews v. the United Kingdom*, application No. 28576/95, Commission decision of 16 October 1996.

[36] "Joint declaration on surveillance programs and their impact on freedom of expression", issued by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, June 2013 (available from www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1), para. 9.

[37] See for example European Court of Human Rights, *Segersted-Wiber and others v. Sweden*, application No. 62332/00, 6 June 2006. See also CCPR/C/21/Rev.1/Add. 13, paras. 15-17.

[38] A/HRC/14/46.

[39] Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law (General Assembly resolution 60/147, annex).

[40] See European Digital Rights, "The Slide from 'Self-Regulation' to Corporate Censorship", Brussels, January 2011, available at www.edri.org/files/EDRI_selfreg_final_20110124.pdf.

43. There may be legitimate reasons for a State to require that an information and communications technology company provide user data; however, when a company supplies data or user information to a State in response to a request that contravenes the right to privacy under international law, a company provides mass surveillance technology or equipment to States without adequate safeguards in place or where the information is otherwise used in violation of human rights, that company risks being complicit in or otherwise involved with human rights abuses. The Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011, provide a global standard for preventing and addressing adverse effects on human rights linked to business activity. The responsibility to respect human rights applies throughout a company's global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations.

44. Important multi-stakeholder efforts have been made to clarify the application of the Guiding Principles in the communications and information technology sector. Enterprises that provide content or Internet services, or supply the technology and equipment that make digital communications possible, for example, should adopt an explicit policy statement outlining their commitment to respect human rights throughout the company's activities. They should also have in place appropriate due diligence policies to identify, assess, prevent and mitigate any adverse impact. Companies should assess whether and how their terms of service, or their policies for gathering and sharing customer data, may result in an adverse impact on the human rights of their users.

45. Where enterprises are faced with government demands for access to data that do not comply with international human rights standards, they are expected to seek to honour the principles of human rights to the greatest extent possible, and to be able to demonstrate their ongoing efforts to do so. This can mean interpreting government demands as narrowly as possible, seeking clarification from a Government with regard to the scope and legal foundation for the demand, requiring a court order before meeting government requests for data, and communicating transparently with users about risks and compliance with government demands. There are positive examples of industry action in this regard, both by individual enterprises and through multi-stakeholder initiatives.

46. A central part of human rights due diligence as defined by the Guiding Principles is meaningful consultation with affected stakeholders. In the context of information and communications technology companies, this also includes ensuring that users have meaningful transparency about how their data are being gathered, stored, used and potentially shared with others, so that they are able to raise concerns and make informed decisions. The Guiding Principles clarify that, where enterprises identify that they have caused or contributed to an adverse human rights impact, they have a responsibility to ensure remediation by providing remedy directly or cooperating with legitimate remedy processes. To enable remediation at the earliest possible stage, enterprises should establish operational-level grievance mechanisms. Such mechanisms may be particularly important in operating countries where rights are not adequately protected or where access to judicial and non-judicial remedies is lacking. In addition to such elements as compensation and restitution, remedy should include information about which data have been shared with State authorities, and how.

V. Conclusions and recommendations

47. **International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data. Practices in many States have, however, revealed a**

lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy.

48. **In addressing the significant gaps in implementation of the right to privacy, two observations are warranted. The first is that information relating to domestic and extraterritorial surveillance policies and practices continues to emerge. Inquiries are ongoing with a view to gather information on electronic surveillance and the collection and storage of personal data, as well as to assess its impact on human rights. Courts at the national and regional levels are engaged in examining the legality of electronic surveillance policies and measures. Any assessment of surveillance policies and practices against international human rights law must necessarily be tempered against the evolving nature of the issue. A second and related observation concerns the disturbing lack of governmental transparency associated with surveillance policies, laws and practices, which hinders any effort to assess their coherence with international human rights law and to ensure accountability.**

49. **Effectively addressing the challenges related to the right to privacy in the context of modern communications technology will require an ongoing, concerted multi-stakeholder engagement. This process should include a dialogue involving all interested stakeholders, including Member States, civil society, scientific and technical communities, the business sector, academics and human rights experts. As communication technologies continue to evolve, leadership will be critical to ensuring that these technologies are used to deliver on their potential towards the improved enjoyment of the human rights enshrined in the international legal framework.**

50. **Bearing the above observations in mind, there is a clear and pressing need for vigilance in ensuring the compliance of any surveillance policy or practice with international human rights law, including the right to privacy, through the development of effective safeguards against abuses. As an immediate measure, States should review their own national laws, policies and practices to ensure full conformity with international human rights law. Where there are shortcomings, States should take steps to address them, including through the adoption of a clear, precise, accessible, comprehensive and non-discriminatory legislative framework. Steps should be taken to ensure that effective and independent oversight regimes and practices are in place, with attention to the right of victims to an effective remedy.**

51. **There are a number of important practical challenges to the promotion and protection of the right to privacy in the digital age. Building upon the initial exploration of some of these issues in the present report, there is a need for further discussion and in-depth study of issues relating to the effective protection of the law, procedural safeguards, effective oversight, and remedies. An in-depth analysis of these issues would help to provide further practical guidance, grounded in international human rights law, on the principles of necessity, proportionality and legitimacy in relation to surveillance practices; on measures for effective, independent and impartial oversight; and on remedial measures. Further analysis also would assist business entities in meeting their responsibility to respect human rights, including due diligence and risk management safeguards, as well as on their role in providing effective remedies.**