United Nations A/HRC/28/39

General Assembly

Distr.: General
19 December 2014

Original: English

Human Rights Council
Twenty-eighth 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

Summary of the Human Rights Council panel discussion on 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 is submitted pursuant to Human Rights Council decision 25/117. It provides a summary of the panel discussion on the right to privacy in the digital age, held on 12 September 2014, during the twenty-seventh session of the Human Rights Council. Based on the request of the Human Rights Council, the promotion and protection of the right to privacy in the digital age in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data, including on a mass scale, also with a view to identifying challenges and best practices, taking into account the report of the United Nations High Commissioner for Human Rights, were examined in the course of the panel discussion.

GE.14-24708 (E)
1424708

Contents

I. Introduction

1. Pursuant to its decision 25/117, the Human Rights Council held a panel discussion on the right to privacy in the digital age on 12 September 2014. The discussion took account of the issues raised in the report of the United Nations High Commissioner for Human Rights submitted to the Human Rights Council at its twenty-seventh session (A/HRC/27/37).

2. Based on the request of the Human Rights Council, the promotion and protection of the right to privacy in the digital age in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data, including on a mass scale, also with a view to identifying challenges and best practices, taking into account the report of the High Commissioner for Human Rights, were examined in the course of the panel discussion.

3. The panel discussion was chaired by the President of the Human Rights Council, and moderated by Marko Milanovic, Associate Professor at Nottingham University. The United Nations Deputy High Commissioner for Human Rights gave an opening address. The panellists were Catalina Botero, Special Rapporteur on freedom of expression, Inter-American Commission on Human Rights, Sarah Cleveland, Louis Henkin Professor of Human and Constitutional Rights, Columbia Law School, Yves Nissim, Deputy Chief Corporate Social Responsibility Officer, Orange, former Chair of the Telecommunications Industry Dialogue, and Carly Nyst, Legal Director, Privacy International.

4. In its decision 25/117, the Council requested the Office of the High Commissioner to present a summary report of the panel discussion at its twenty-eighth session. The present report is submitted pursuant to that request.

II. Opening statement by the United Nations Deputy High Commissioner for Human Rights

5. The Deputy High Commissioner noted that, in a very short space of time, digital communications technologies had revolutionized the way human beings interact and that for millions of people, the digital age was one of emancipation – perhaps the greatest liberation movement the world had ever known. She noted as an example that over one million people had participated electronically in the open dialogue and consultation that was conducted to develop a framework for the post-2015 sustainable development goals, which called for the full inclusion of human rights. She emphasized that human rights defenders, activists, democratic voices, minorities and others could now communicate via digital platforms and participate in the global debate in ways that were previously inconceivable.

6. The Deputy High Commissioner also noted that those digital platforms were vulnerable to surveillance, interception and data collection. Deep concerns had been expressed, as policies and practices that exploited that vulnerability had been exposed across the globe. She added that surveillance practices could have a very real impact on peoples' human rights, including their rights to privacy to freedom of expression and opinion, to freedom of assembly, to family life and to health. In particular, information collected through digital surveillance had been used to target dissidents and there were credible reports suggesting that digital technologies had been used to gather information that led to torture and other forms of ill-treatment.

7. The Deputy High Commissioner recalled that in resolution 68/167, the General Assembly had requested the High Commissioner 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", which was presented to the Human Rights Council at its twenty-seventh session. The report built on expert consultations and in-depth research regarding existing national and international legislation and jurisprudence, and information from a broad range of sources, including replies to a questionnaire sent out to stakeholders.

8. As the report made clear, international human rights law provided a robust 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. However, practices in many States revealed a lack of adequate national legislation and enforcement, weak procedural safeguards and ineffective oversight, which contributed to widespread impunity for arbitrary or unlawful interference with the right to privacy.

9. The Deputy High Commissioner recalled that the High Commissioner's report examined the protection afforded by international human rights law regarding privacy, including the meaning of "interference with privacy" in online communications; the definition of "arbitrary and unlawful" interference in that context; and the question of whose rights were protected, and where. For instance, on the question of what constituted privacy interference, it was clear that the aggregation of communications data might give a comprehensive insight into an individual's behaviour, social relationships, private preferences and identity, extending even beyond the information obtained by reading someone's mail. The collection and retention of communications data might therefore constitute an interference with privacy, whether or not those data were subsequently consulted or used. The very existence of a mass surveillance programme regarding email communication and other forms of digital expression created an interference with privacy, and the onus was on the State to demonstrate that such interference was neither unlawful nor arbitrary.

10. Turning to "arbitrary" or "unlawful" interference with privacy, the report noted that State surveillance of electronic communications data might be a legitimate law enforcement measure, if it was conducted in compliance with the law. But States must demonstrate that the surveillance was both necessary and proportionate to the specific risk being addressed. Mandatory third-party data retention – whereby telephone companies and Internet service providers were required to store metadata about communications by their customers, for subsequent access by law enforcement and intelligence agencies – appeared neither necessary nor proportionate.

11. As stressed in the report, the Deputy High Commissioner recalled that States had an obligation to ensure that the privacy of individuals was protected by law against unlawful or arbitrary interference. All forms of communications surveillance must be conducted on the basis of publicly accessible law; and that law must in turn comply with the constitutional regime of the State concerned and international human rights law. Secret rules and secret interpretations of the law – even if issued by judges – were not compatible with the principle that laws should be clear and accessible. Neither were laws or rules that gave excessive discretion to executive authorities, such as the security and intelligence services.

12. The Deputy High Commissioner also mentioned the concerns raised in the report regarding extraterritorial surveillance and the interception of digital communications. Drawing on the work of the Human Rights Committee and the International Court of Justice regarding the determination of when a State exercises jurisdiction, the report noted that the human rights obligations of a State were engaged whenever it exercised power or

effective control. If surveillance involved the exercise of power or effective control by a State in relation to digital communications infrastructure, then wherever it might be taking place, that surveillance might engage the human rights obligations of the State. That would include, for example, direct tapping or penetration of a communications infrastructure and exercise by the State of regulatory jurisdiction over a third party which physically controlled the data.

13. The report recalled that international human rights law was also explicit on the principle of non-discrimination and that States must take measures to ensure that any interference with the right to privacy complied with the principles of legality, proportionality and necessity, regardless of the ethnicity, nationality, location or other status of the people whose communications it was monitoring.

14. The report also referred to the essential nature of procedural safeguards and effective oversight to safeguard the right to privacy in law and in practice. A lack of effective oversight had contributed to impunity for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Internal safeguards devoid of independent oversight had been demonstrably ineffective against unlawful or arbitrary surveillance methods. Appropriate safeguards must include independent civilian oversight and participation from all branches of Government, in order to ensure the effective protection of the law. States also had a legal obligation to provide effective remedies for violations of privacy through digital surveillance, in judicial, legislative or administrative forms, with procedures that were known and accessible.

15. Finally, the Deputy High Commissioner referred to the role of the private sector, an issue also addressed in the report of the High Commissioner. Governments increasingly relied on corporations to conduct and facilitate digital surveillance. In some cases there might be legitimate reasons for a company to provide user data. But when the request was in violation of human rights law, or where the information was used in violation of human rights law, that company risked being complicit in human rights abuses. The Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in resolution 17/4 of 16 June 2011, provided a global standard for preventing and addressing adverse the human rights effects of business activity. They made clear that the responsibility to protect human rights applied throughout a company's global operations, regardless of where its users were located, and independently of whether a State met its own human rights obligations. Many corporations appeared to be insufficiently aware of those issues.

16. The Deputy High Commissioner concluded by noting that the lack of government transparency regarding the measures that they had adopted that might impact on the right to privacy, often rendered attempts to address the gaps and exercise accountability extremely arduous. She concluded that there was a clear need for further discussion and in-depth analysis as information regarding those measures became public.

III. Contributions of panellists

17. In response to questions from the moderator, the initial remarks of the panellists focused on issues linked to the international human rights law framework with respect to the right to privacy, including procedural safeguards, effective oversight and right to a remedy, as well as the role of the business sector.

18. The Legal Director at Privacy International highlighted the importance of privacy in any democratic society and stressed the links between privacy and the concept of human dignity. She noted that the right to privacy was a fundamental precondition to, and guarantor of, other rights, as it enabled individuals to independently develop thoughts and

ideas that could be freely expressed, to choose which religion in which to worship and which political party to support. Ms. Nyst explained that the right to privacy was first articulated in international law in the Universal Declaration of Human Rights, when the drafters were clear not only about the necessity of the inclusion of the right to privacy, but also about the importance of the right to privacy of communications, as shown by the *travaux preparatoires* to the Declaration.

19. Ms. Nyst noted that many common actions done on a daily basis included a "communication", such as sending an e-mail or a text message, accessing a bank account, searching for information on the Internet, or accessing government services. Any digital communication involved private data travelling around the world, and through the cables of many private companies, before it reached its destination. The challenge that technology posed to privacy was to ensure that the obligations of the State to respect, fulfil and protect the right to privacy and the responsibilities of the private sector were meaningful in the digital era. She noted that the legal framework already existed, as the right to privacy was enshrined in most international and regional human rights treaties and in many national constitutions, and that a new understanding of how those texts applied was needed.

20. The Special Rapporteur on freedom of expression of the Inter-American Commission on Human Rights referred to the opportunities for the free expression, communication and exchange of information created by the Internet. She noted that, at the same time, the capture, storage, and administration of enormous quantities of data had also been facilitated. That information, whether content data or metadata, could be highly revealing of even the most intimate aspects of the private lives of individuals or communities. She noted that legal frameworks had not followed the pace of technological developments in the digital era, and stressed the need for regulation of both the collection and analysis of information, taking into account freedom of expression, the right to privacy and other relevant human rights.

21. Ms. Botero further noted that surveillance policies could have an impact on a broad spectrum of human rights. She referred to the impact of surveillance on the right to freedom of expression, either directly when the right could not be exercised anonymously as a consequence of surveillance, or indirectly, because the mere existence of surveillance could have a chilling effect, instil fear and inhibition and make individuals cautious about what they said and did. She explained that, because the right to freedom of expression was a platform right, its violation could also lead to the violation of other rights, including freedom of association, freedom of assembly, religious freedoms and the right to health. Because of the potential impact of surveillance activities on the entire human rights architecture, there was a need for States to revise their laws to establish limits on surveillance programmes, which should include respect for the principles of necessity and proportionality, and appropriate monitoring mechanisms. Ms. Botero explained that because the Internet was a special and unique communications medium that enabled the free, plural, and democratic exercise of the right to freedom of expression, its governance was a particularly relevant matter. She noted that in order to make sure that all relevant points of view could be properly considered, States must ensure the equal participation of all actors relevant to the governance of the Internet and foster strengthened cooperation between the authorities, academia, civil society, the scientific and technical communities and the private sector, both nationally and internationally.

22. The Louis Henkin Professor of Human and Constitutional Rights at Columbia Law School stated that all persons, regardless of location or nationality, were protected by human rights that were universal and inherent to human dignity. She noted that State surveillance practices sometimes distinguished between citizens and non-citizens. In that regard, Ms. Cleveland stressed that, as recognized by the Human Rights Committee, the principle of non-discrimination in article 2 of the International Covenant on Civil and

Political Rights protected citizens and non-citizens alike.[1] Consequently, neither citizens nor non-citizens might be subjected to unlawful or arbitrary interference with their privacy. She also noted that surveillance was often undertaken by States on their own territory, to suppress freedom of expression and association, or to punish journalists, dissidents and other government critics. According to article 17 of the International Covenant on Civil and Political Rights, States had the obligation to respect and ensure the privacy rights of all persons within their territory and subject to their jurisdiction.

23. Ms. Cleveland emphasized that the protections in the International Covenant on Civil and Political Rights applied to persons otherwise subject to the jurisdiction of a State, as recognized by the International Court of Justice[2] and the Human Rights Committee.[3] That was also the reading that best reconciled the text of the International Covenant on Civil and Political Rights with its content, object and purpose. The Human Rights Committee had long recognized that a State could not avoid its international human rights obligations by taking action outside its territory that it would be prohibited from taking at home. Ms. Cleveland explained that cyber activity transcended territory, that digital surveillance could involve the minimal exercise of physical control by the State over a person or territory and could involve action in one location that had an impact upon a person in another. She stressed that such conduct could engage the human rights obligations of a State. Lastly, she noted that the fact that privacy rights applied to non-citizens or nationals abroad did not mean that surveillance activities were per se always unlawful. Any restriction to the right to privacy to accommodate legitimate national security or law enforcement interests must be adopted while taking full account of the requirements, as provided in international human rights law; in particular they must not be arbitrary or unlawful.

24. Turning to the role of the private sector, the moderator, Mr. Milanovic, noted that private companies aggregated data for their own purposes, and might also be co-opted into governmental schemes. Focussing on the relationship between Governments and private telecommunication companies, he asked how private companies should react to government requests. The Deputy Chief Corporate Social Responsibility Officer at Orange noted that issues relating to various requests that a telecommunication company might receive to collect or keep data regarding their customers or to make their networks "wiretap-ready" became more vivid during the Arab Spring. Telecommunication companies had received requests from Governments – in some cases at gunpoint – that might have had an impact on the the rights to freedom of expression and privacy of their customers. That had led those companies to create the Telecommunications Industry Dialogue on Freedom of Expression and Privacy, to jointly address issues related to freedom of expression and the right to privacy in the telecommunications sector.[4] The Dialogue had published a set of 10 guiding principles on 12 March 2013, which were influenced by the Guiding Principles on Business and Human Rights: implementing the United Nations "Protect, Respect and Remedy" Framework. The principles published by the Dialogue addressed privacy and freedom of expression as they related to the telecommunications sector, specifically exploring the

[1] See Human Rights Committee, general comment No. 18 (1989) on non-discrimination.

[2] See International Court of Justice, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004,* p. 136., and *Armed Activities on the Territory of the Congo* (*Democratic Republic of the Congo* v. *Uganda*), *Judgment, I.C.J. Reports 2005*, p. 168.

[3] See Human Rights Committee, general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the Covenant.

[4] The Telecommunications Industry Dialogue is currently composed of seven operators and two vendors. See www.telecomindustrydialogue.org.

interaction and boundaries between the duty of a Government to protect human rights and the responsibility of telecommunications companies to respect human rights.

25. In terms of challenges, Mr. Nissim emphasized that telecommunications companies had many personnel on the ground in various countries and that their safety and security was an absolute priority, as recognized in the fifth guiding principle.[5] He also noted that, while the companies engaged in the Telecommunications Industry Dialogue wanted to uphold human rights, in particular freedom of expression and the right to privacy, it was important to recall that they had licence agreements with Governments and were subject to national laws and regulations. Because of the need to protect their staff who were present in-country, companies needed to be able to engage in a dialogue with host Governments whenever necessary. He noted that there were three pressing issues that needed to be resolved. First, Governments should not request or be granted direct access to the telecommunications network. Second, the process through which Governments could make requests to telecommunications companies must be clear and transparent. Third, while telecommunications companies were willing to be transparent about the requests they received, transparency was the responsibility first and foremost of Governments.

26. Turning to the conditions for the lawful restriction of the right to privacy and freedom of expression, Ms. Botero explained that any limitation must be established beforehand by legislation. Such laws must precisely define the causes and conditions that would enable the State to intercept the communications of individuals, collect communications data or subject them to surveillance or monitoring that had an impact on the right to privacy. The law must not be vague or ambiguous, or grant broad discretionary powers to the executive power in its interpretation. It must also provide safeguards pertaining to the nature, scope and duration of surveillance measures. Limitations to the right to privacy must also pursue a legitimate aim. In the case of surveillance, the grounds most likely to be relied upon by the State were national security and the fight against crime. Any limitation must be proportionate and strictly necessary. That means that a true and compelling need to impose the limitation must be clearly established and the objective could not be accomplished by any other less restrictive measure. In any event, the rights should be limited only when the risk to the protected interest, narrowly defined, was greater than the general interest in maintaining the right to privacy and freedom of expression. Ms. Botero also noted that the test must be stronger when the rights protected dealt with the most intimate aspects of a person's private life. In order to ensure the protection of the principles of legality, proportionality and necessity, decisions to undertake surveillance activities that limited the right to privacy and other rights should be authorized by independent judicial authorities.

27. With regard to proportionality, Ms. Cleveland noted that a measure should be proportionate to the significance of the interests at stake: the interest of the State in pursuing the measure and the privacy interest of the individual. She explained that the more acute the privacy interest of the individual, the more narrowly tailored the measure must be. She referred to the jurisprudence of the European Court of Human Rights, which provided a reasonable margin of appreciation to States, especially in the national security area, to determine on a case-by-case basis what measures were necessary and proportionate to the achievement of a particular State interest. Ms. Cleveland also noted the importance of the procedural safeguards put in place by the State to ensure that the surveillance regime was being applied properly. She noted that there needed to be legal safeguards to define the

[5] Principle 5 states "Always seek to ensure the safety and liberty of company personnel who may be placed at risk".

regime, as well as oversight and remedies ex post facto to make sure that the regime was not abused.

28. Mr. Milanovic noted that States often made a distinction between the collection of the content of a communication, on the one hand, and data about the communication, or metadata, on the other, with the former subject to stronger safeguards than the latter. He asked whether such distinctions were relevant regarding digital communications. Ms. Nyst noted that such distinctions must be unequivocally abandoned, as they reflected an outdated understanding of the nature of today's communications and a failure to update laws accordingly. She noted that such distinctions dated back to an era where there was indeed a difference between the envelope and the content of the envelope, whereas when looking at digital communications, the so-called envelope, or metadata, contained very sensitive, valuable and extensive information. For instance, that information could be derived from the metadata and analysed to obtain information about an individual's political or religious beliefs. She referred to a study by Stanford University, which showed that medical, financial and legal information could be obtained from metadata. She stressed the serious need, therefore, to re-evaluate that distinction, as noted in the report of the High Commissioner. Ms. Nyst noted progress in several countries, which had recognized the need for increased protection of metadata. She also noted that the European Court of Justice had recently invalidated the blanket data retention law[6] and concluded that there was a trend towards increased protection of metadata. However, Ms. Nyst stressed that further guidance on how domestic laws should follow suit was needed.

29. From an operator's perspective, Mr. Nissim said that data such as tracking calls was often retained by telecommunications companies for technical reasons, to ensure the quality of services and networks. He noted, however, that when Governments asked telecommunications companies to retain the information collected for longer periods of time, or to provide access, the information could be misused. He added that any access by Governments should require legislation. Mr. Nissim also noted that where the level of "big data" was reached, and if the information was anonymized, it could be used in a very positive way, e.g. for urban planning, transportation and communications.

IV. Summary of the discussion

30. During the interactive discussion, delegations from Algeria, Australia, Belgium, Canada, China, Cuba (on behalf of the like-minded group of countries), Ecuador, the European Union, Estonia, France, Germany (on behalf of Austria, Brazil, Germany, Liechtenstein, Mexico, the Netherlands, Norway and Switzerland), India, Indonesia, Ireland, Italy, Malaysia, Pakistan (on behalf of the Organization of Islamic Cooperation), Romania, the Russian Federation, Sierra Leone, Slovenia, the United Arab Emirates, the United Kingdom of Great Britain and Northern Ireland, the United States of America, the Bolivarian Republic of Venezuela and the United Nations Educational, Scientific and Cultural Organization (UNESCO) took the floor. Statements by Chile, Myanmar and Uruguay were not delivered due to lack of time. Copies of their statements were posted on the Human Rights Council extranet.

31. Delegates of the following non-governmental organizations also took the floor: the American Civil Liberties Union (in a joint statement with Human Rights Watch), Article 19, the Association for Progressive Communications and the Korea Center for United Nations Human Rights Policy.

[6] See European Court of Justice, judgement of 8 April 2014, joined cases C-293/12 and C-594/12.

A. General remarks on the right to privacy in the digital age

32. Many delegations highlighted the quality of the report submitted by the High Commissioner on the right to privacy in the digital age and the fact that it was an important milestone in the context of the ongoing discussion. Many delegations also noted their appreciation for the work of the Office of the United Nations High Commissioner for Human Rights (OHCHR) and others in ensuring that the right to privacy was safeguarded in law and in practice.

33. Many delegations welcomed the panel discussion, as the topic was timely and the discussion necessary, bearing in mind that technological advances ran ahead of an understanding of their human rights implications. The importance of discussions held on the issue by the Human Rights Council, as well as in other forums, such as the Internet Governance Forum, was also noted.

34. One delegation noted that there were close to 3 billion Internet users around the world and that a free and secure Internet had become a priority for people everywhere. As foreseen in the post-2015 sustainable development goals and the Programme of Action for the Least Developed Countries for the Decade 2011–2020 (A/CONF.219/3/Rev.1), everyone should have access to the Internet by 2020.

35. Most interventions indicated, as already highlighted in the report of the United Nations High Commissioner, that innovations in technology had had a positive impact on freedom of expression, had facilitated global debate and had fostered democratic participation. It was noted that digital communications could be tools for facilitating the enjoyment of human rights, had contributed to the advancement of human civilization, and had brought new opportunities for communication, knowledge and business. Privacy was integral to a free, fair and open society in which views could be freely expressed without any fear of repression or detention.

36. Most delegations noted, however, that the same technological platforms had also enhanced the capacities of State and non-State actors to conduct surveillance, interception and mass data collection. Some delegations stated that those platforms were not only vulnerable to mass surveillance, but actually facilitated it. One NGO noted that when privacy online was threatened, trust in the Internet disappeared, depriving everyone, including journalists, bloggers and human rights defenders, of the liberty to communicate securely, anonymously and in confidence, with a chilling effect on freedom of expression. Another NGO emphasized that for everyone, especially those living under repressive regimes, the integrity of communications was critical to preserving individual liberty and security of the person, as well as political rights.

37. The exponential growth of State power in some countries due to their information technology infrastructure was noted. Some delegations focused on the fact that much of the world's electronic communications passed through a limited number of countries. In turn, that provided an opportunity for intercepting private communications. Some countries had developed technologies that allowed access to much of the world's global Internet traffic, call records, individuals' electronic address books and huge volumes of other digital communications content. Reports of certain Governments monitoring communications at global events were also referred to. A number of speakers recalled that the sovereignty of States should always be respected with regard to surveillance, interception and the collection of personal data.

38. Other delegations noted that there was a growing trend by some Governments to use cybertechnologies to control their own citizens, in violation of their right to freedom of expression and the right of access to information. It was noted that political activists and members of religious minorities were targeted, detained and sometimes killed. An NGO

noted that the effects of online surveillance were often felt offline and were part of a global trend to restrict civic space. Lawful protest movements were monitored by the State and private actors to undermine peaceful actions and related rights, in particular the rights to freedom of expression and assembly.

39. Most delegations reaffirmed that rights held by people offline must also be protected online, as set out in General Assembly resolution 68/167 and Human Rights Council resolutions 20/8 and 26/13.

40. Most delegations considered the right to privacy a precondition to being able to freely express oneself and one of the founding rights of a democratic society. Many delegations noted that surveillance had an impact on rights other than the right to privacy, in particular freedom of expression and of opinion and freedom of assembly and association. It was further noted that privacy and freedom of expression were "interlinked and mutually dependent" (see A/HRC/23/40, para. 79) and that they enabled and facilitated the development of other fundamental rights and sustainable development. To illustrate this, two NGOs noted the concrete harm that large-scale electronic surveillance could have on the work of journalists and lawyers, undermining freedom of expression and association and the right to counsel.[7] One delegation referred to attempts to silence the media. Another NGO referred to bloggers facing charges of terrorism, partly because they had encrypted their communications and engaged in digital security training to ensure their privacy.

41. One delegation noted that individuals were often not aware of the extent to which data could be used or shared, even when collected with their consent. Some delegations referred to the right to data protection and to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional Protocol as the first binding international instrument in the data protection field and an important contribution to the right to privacy. One delegation referred to a so-called "right to be forgotten", where the legitimate wish not to be associated with only a particular aspect of one's life or past might clash with the right to be informed and might also lead to a distortion in collective memory.

42. Many delegations highlighted the measures taken at national level to ensure protection of the right to privacy in the digital age. UNESCO referred to its work in relation to privacy and freedom of expression in the digital age, to a publication on internet privacy and freedom and expression and to a comprehensive study on Internet issues, including a focus on freedom of expression, privacy, access to knowledge and information and the ethics of the information society.

B. Legal protection of the right to privacy

43. Most delegations emphasized that international law provided a clear framework for the right to privacy, enshrined in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights. Many observed, however, that the implementation of the right to privacy was lacking and that there was a need for concrete measures to safeguard that right. Some noted that unilateral and unauthorized access to private data and extensive surveillance needed to be addressed comprehensively and calls were made for urgent measures to be taken to stop current surveillance practices and protect individuals from violations of their right to privacy.

[7] Human Rights Watch and American Civil Liberties Union, "With liberty to monitor all: how large-scale US surveillance is harming journalism, law and American democracy" (July 2014).

44. Many delegations recalled that any limitation to the right to privacy must be based on accessible, transparent, clear, comprehensive and non-discriminatory laws and be limited to what was necessary to safeguard the public interest in a democratic society. Any state surveillance of individuals must be proportionate and fair, in compliance with international norms and standards, governed by the rule of law and subject to oversight. There must be adequate and effective guarantees against abuses. It was noted that defining the line between arbitrary or unlawful interference in the right to privacy properly would be one of the challenges of the next few years. It was also stressed that blanket surveillance could amount to an unjustified infringement. One delegation noted that article 17 of the Covenant must be the basis for discussion of the limiting principles – legality and arbitrariness – expressly stated therein.

45. Several delegations noted that States had legitimate security concerns, including the threat of terrorism and cybercrime. One delegation noted that the use of the Internet for criminal and antisocial activities was on the rise. Another delegation noted that security required intelligence, including with regard to digital communications to counter terrorism, while another stated that Governments had the responsibility to protect individuals, and that data surveillance could be an effective and legitimate measure for law enforcement purposes. There was broad agreement, however, that legitimate security concerns needed to be addressed within the framework of international human rights law, including the right to privacy.

46. In response to a question about data-sharing between government agencies, Ms. Nyst stated that the same oversight and procedural guarantees should apply to information collected directly and obtained through the sharing of information. Ms. Cleveland noted that the Human Rights Committee had expressed concern in that regard.[8] Data sharing between various State agencies within a given country could be legitimate, provided the purpose of the collection and use of that data was the same for each of those agencies, so as to ensure compliance with the principles of necessity and proportionality and therefore no breach of the right to privacy.

47. Some delegations noted that the Internet transcended traditionally existing geographical boundaries. Several delegations recalled that, as stated in the report of the High Commissioner, human rights law applied when a State exercised power outside its own territory, so that it could not avoid its international human rights obligations and bypass its own national laws by taking action outside its territory, which it would be prohibited from taking at home. Several delegations recalled that article 17 of the International Covenant on Civil and Political Rights must be read in conjunction with article 2 of the Covenant, which states that the obligations of States apply to all individuals within their territory and subject to their jurisdiction. Several delegations noted that any interference with the right to privacy should comply with the principles of legality, proportionality and necessity, regardless of the nationality or location of individuals whose communications are under direct surveillance. While many delegations stressed that the responsibility of the State to protect the right to privacy did not end at its borders, some delegations expressed concerns about expansive views on the extraterritorial application of the Covenant and called for an in-depth discussion on the issue of extraterritoriality with regard to article 17.

48. Ms. Nyst recalled that most surveillance took place within a State. On the question of citizenship-based distinctions for the purpose of surveillance, she noted that not only were those distinctions in violation of the principle of non-discrimination, but it was also a very outdated and impractical approach, because it was difficult – if not impossible – to

[8] See Human Rights Committee general comment No. 16 (1988) on the right to privacy, para. 10.

know the nationality of the sender of a digital communication. On the question of whether control over telecommunications infrastructure could qualify as State jurisdiction for the purposes of article 2 of the Covenant, Ms. Cleveland stated that because digital communication transcended geography, some conception of the extraterritorial application of human rights was necessary to ensure that human rights could be protected online as well as offline. She noted that there were various approaches to extraterritoriality, most of which focused on the concept of jurisdiction outside the territory as involving some form of effective control over a person or a territory, and that under that approach, it was possible to view the exercise of control over Internet infrastructure as the exercise of control over a territory that had effects on the rights of individuals, wherever they might be located.

49. It was noted that the responsibility to respect the right to privacy lay with a number of different actors. Some delegations underscored the lack of effective oversight as having contributed to a lack of accountability for unlawful intrusions on the right to privacy, as well as the shortcomings of relying on internal safeguards without independent external monitoring. The need to protect the rights of victims was underlined. One delegation noted that it was up to each State to develop independent and effective national oversight mechanisms, to ensure the proper application of the rules that govern electronic surveillance. One non-governmental organisation stated that there had been cases of mass surveillance for the purpose of arresting human rights defenders or identifying participants at peaceful assemblies, where "rubber stamping" by the courts had been instrumental, or where personal data collected by telecommunication companies through real-name verification systems had been provided to intelligence and investigative agencies in the absence of any court examination. The need for effective oversight regimes, with attention paid to the rights of victims to an effective remedy, was stressed, including the involvement of an independent and impartial judiciary as a key safeguard.

50. In response to questions about procedural safeguards and oversight mechanisms to ensure that the law was effective and applied in practice, Ms. Nyst explained that an essential precondition to greater and more effective oversight was the end to pervasive secrecy. Governments needed to be more transparent about the activities they needed to engage in to provide security and they must not compromise the infrastructure in a way that was beyond control of the public. She also noted that all individuals, particularly judges and lawyers, should gain a better understanding of how Internet technology worked, which would help them to better understand how surveillance worked. She underscored the importance of ensuring that any surveillance was authorized by an independent and competent judicial authority. She added that it was essential that individuals be notified of the fact that they had been subject to surveillance, in order to be in a position to obtain redress. She also noted the need for more rigorous independent oversight mechanisms, with technical understanding of how surveillance worked, to enable an examination to be made of the human rights implications of surveillance by the security services. Finally, she noted that a special procedures mandate holder with technical expertise could provide guidance about good practices and about what the human rights framework required to ensure the protection of the right to privacy. Ms. Botero added that there was no uniformity in the domestic standards that regulated surveillance and said that a good practice at national level was to have an expert body that would focus specifically on technology and human rights in the context of surveillance. She noted that oversight could be institutional, judicial, inter-organic and through an ombudsperson, that procedural guarantees should include prior judicial authorization of surveillance measures and that the legal basis and criteria for the decision should be public.

51. Turning to a question on the obligation of States to provide an effective remedy for violations of the right to privacy, Ms. Cleveland noted that while article 2 of the International Covenant on Civil and Political Rights provided an obligation for States to grant an effective remedy, this was a very difficult question, owing to the secrecy of

surveillance practices. Individuals often did not know that they had been subject to surveillance and therefore might lack standing because they could not show sufficient injury. She noted that Governments needed to be more transparent about the surveillance programmes that they were pursuing, to allow for public scrutiny. She also noted that it was important that individuals received specific notice that they had been subject to surveillance after the surveillance had ceased. She further noted that standing rules must be generous enough to allow for meaningful challenge of surveillance programmes. In that respect, she emphasized that the European Court of Human Rights required a sufficient likelihood – not a demonstration – of actual injury. She noted that classified judicial proceedings were problematic, but that some kind of judicial test was nonetheless important. The key challenge was to make those proceedings as transparent and effective as possible.

52. On the question of whether there should be dedicated courts to examine surveillance measures, Ms. Cleveland noted that States needed to find a way to satisfy transparency requirements and democratic oversight, while at the same time allowing for some level of confidentiality. A good option was to have special procedures to deal with classified information, but in regular courts. On that point, Ms. Nyst added that while there was some value in having specialized judges with technical knowledge, it was essential that courts allowed parties to be on an equal footing when challenging surveillance. It was crucial, therefore, that there be no secret courts and no procedure that would allow for secret interpretations of laws. Any court that did not allow for the utmost transparency and scrutiny did not allow the power asymmetry between the individual and the State to be corrected and might in fact serve to legitimize unlawful surveillance measures.

C. Specific issues regarding business entities

53. The role of private companies was also raised by several delegations. Some delegations noted that companies had been put under pressure by Governments, or had been compelled to hand over data. Others noted that international Internet and telecommunication technology companies had been developing and executing their own surveillance capabilities or assisting States in their surveillance of individuals. Mr. Nissim noted that the technology used by telecommunications companies was very complicated, but could be accessed by Governments. He referred for example to "deep packet inspection", which enabled the content of communications to be examined as it was transmitted and thereby allowed Internet service providers to monitor and analyse the Internet communications of users in real time. Mr. Nissim noted that this equipment was used by telecommunication companies to improve the service that they provided to customers, but that it could also be used by Governments for surveillance purposes, without the telecommunication company even being aware of what was happening, as had happened to Orange in the course of its operations.[9]

54. Many delegations asked that businesses and third parties be more transparent and accountable in their conduct. Some delegations emphasized that a deeper understanding of how intermediaries and other business entities could meet their responsibilities to respect human rights, as well as the identification of the regulatory powers which ought to rest with the public and the private sector, was necessary. Mr. Nissim confirmed that transparency was a key issue for telecommunication companies that were under severe pressure to be more transparent. In that regard, he noted that his chief executive of his company had signed a data protection charter, which committed the company to protecting the security of

[9] See Human Rights Watch, "They know everything we do: telecom and Internet surveillance in Ethiopia" (March 2014).

its customers' personal data; providing control for customers over their own personal data and how it was used; being transparent in terms of the handling of data for its customers and users at all stages; and providing support for all its customers and users to help them protect their privacy and manage their personal data. He noted however, that his company had suffered two breaches of privacy since the charter was signed, emphasizing that protecting data from government interference was always a challenge. He stated again that it was important to recall that, while a number of telecommunication companies were committed to being transparent, transparency must come, first and foremost, from the State. He also recalled that telecommunication companies were bound by local laws and therefore that the legal framework within which they operated varied from country to country. He noted an ongoing trend for companies to map the legal framework in all the countries in which they operated. He noted that in some countries, the legislation allowed for transparency ex-post facto, either by allowing the companies to provide information on the requests made to them by Governments, or the data transmitted to them, or by permitting the State to do so. In other States, neither the company nor the State could be transparent about the measures the company had had to share. He noted that telecommunications companies tried with the means at their disposal to protect international human rights law. For example, he noted that during the Arab Spring, a Government had requested his company to send text messages to all their base customers. Following an initial refusal from the company, members of the armed forces were sent to reiterate the demands of the Government. His company sent the message as requested, together with the signature of one of the members of the armed forces present. This was a small, yet important, piece of information, which allowed civil society to understand the situation.

55. Mr. Nissim highlighted the importance of multi-stakeholder engagement. In order to illustrate that point, he referred to another situation which his own company had faced, where the Government in question had backed down on the requests it had made to telecommunication companies, owing to several factors, one of them being the fact that civil society had publicized those requests. He noted that he would support the elaboration of a legal instrument at the international level that would deal with the obligations of private entities regarding protection of the right to privacy from surveillance measures, and that model laws and best practices would also greatly assist Governments.

D. Way forward

56. Many delegations stressed the need for continued multi-stakeholder engagement. They said that State engagement was not enough, but that private entities, civil society, scientific and technical communities, the business sector, academics and human rights experts needed to take part in the discussions. The need for further engagement of the Human Rights Council was also highlighted.

57. Several delegations requested that States review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data, in order to adapt them to the needs of the twenty-first century and to ensure that they were in full conformity with international human rights law. Others called for a transparent international system with an adequate international framework of Internet governance, including appropriate safeguards to protect personal data. One delegation called for the development of a code of conduct on those issues. Several delegations and NGOs called upon the Council to establish a mandate for a special rapporteur on the right to privacy, as it was essential to bring focused and sustained attention to those issues.

V. Conclusions

58. **Panellists concluded that technological change might pose new challenges to existing legislation. In such cases, established legal frameworks, including international human rights law, would continue to apply, even if the implementation of the law must be adapted to address the new reality. Regarding the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, the international human rights framework was clear. There was a need, however, for better implementation at the national level of the international norms related to the right to privacy, through adequate national legislation and stronger safeguards and oversight.**

59. **Panellists noted that the development of legal safeguards against violations and effective oversight involving all stakeholders was essential. Independent, impartial and competent courts must be more involved and better equipped to deal with those complex issues. Furthermore, they noted the need for increased transparency, regarding both surveillance policies and legislation and legal interpretations and court rulings, where they existed. The laws and regulations and the way they were interpreted and applied should be made publicly available. The powers of Governments to access communication-related data should be based on a clear and transparent legal framework that accommodated advances in technology and was in accordance with the rule of law and international human rights norms and standards.**

60. **Supporting the views of States, regional organizations and NGOs, the panellists stressed that the protection and promotion of, and respect for, the right to privacy required the sustained engagement of all stakeholders, including Governments, industry, civil society and international organizations. They highlighted the unique ability of the United Nations to convene all stakeholders and to explore the most effective means of protecting the right to privacy and emphasized that the Human Rights Council should continue to address the issue, including through the universal periodic review, with the increased engagement of civil society. OHCHR and the High Commissioner should also continue to work on the issue and special procedures must engage within their own mandates as appropriate, Consideration should also be given to the need to establish a new special procedures mandate on the right to privacy, to examine existing challenges and how the right should be conceptualized more broadly.**

61. **Finally, the panellists highlighted the vital role played by the United Nations and other international organizations in promoting the international legal standards that guide the actions of private companies, as they seek to respect the human rights of their customers and other users. Businesses look to the United Nations for support in promoting the adoption of those standards in the domestic law of Member States. By furthering the international framework, international organizations were also supporting businesses in meeting their responsibility to respect and protect the privacy of users, as technological advances continued. The question of whether a model law or a code of conduct could be drafted should be considered.**