United Nations A/HRC/41/35/Add.4

General Assembly

Distr.: General
27 May 2019

English only

Human Rights Council
Forty-first session
24 June–12 July 2019
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Summary of an Experts consultation on A/HRC/41/35

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*

Summary

The Secretariat has the honour to transmit to the Human Rights Council an addendum to the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, pursuant to Council resolution 34/18. In his report the Special Rapporteur evaluates the private surveillance industry and the use of its products in violation of rights guaranteed under international human rights law.

* The present document is being issued without formal editing.

GE.19-08635(E)

1908635

Summary of an Experts consultation on A/HRC/41/35 - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Contents

I. Introduction

1. Surveillance technologies are increasingly used by governments around the world to monitor and interfere with the private communications of activists, journalists, academics, opposition figures, dissenters and other figures in civil society. While mass surveillance (i.e. bulk collection of intercepted communications) has been on the global policy agenda at least since the revelations of Edward Snowden in 2013, comparatively less attention – whether press, legislative or regulatory – has been devoted to targeted surveillance using the increasingly available tools developed and marketed by private industry. Yet there is virtually no oversight of the work of these companies, which operate in the shadows of government and inter-governmental activity. While government surveillance is often targeted at civil society in their own states, the surveillance may often have cross-border impact. State surveillance and attack can have a particular chilling effect on members of civil society organizations such as journalists, activists, and academics, ultimately deterring the free expression of information and ideas.

II. Objectives

2. The overall objective of this consultation was to discuss and better understand the threat to individual rights and civic space that stems from the collaboration between private surveillance companies and governments with the involvement of experts in the field of surveillance, targets of surveillance and related threats. More specifically, this consultation allowed participants to:

3. Explore different types of surveillance tools, how they are marketed, sold, and regulated, how governments utilize private surveillance mechanisms, and how civil society can be empowered to respond.

4. Address a major gap in legal frameworks, at the domestic, regional and international level, concerning the control and use of such technologies.

5. Discuss the development of rights-oriented approaches to address the responsibility of state actors and private actors, and the regulation of the surveillance tools they produce.

6. Prepare upcoming reports of the UN Special Rapporteur on freedom of expression and opinion and the UN Special Rapporteur on freedom of association and peaceful assembly that will explore this important issue and the role that the international community may play in developing international standards in this space.

III. Background/Participants

7. The meeting involved a diverse and tech-savvy group of participants, many of them with a solid background in human rights law and/or surveillance technologies. Participants were carefully selected depending on their expertise in the control of surveillance technologies and ability to enrich the discussions with different perspectives. It brought together 19 experts coming from Cambodia, Canada, Chile, Italy, India, Germany, Malaysia, Mexico, Nigeria, Philippines, Sweden, Thailand, United Kingdom and the United States. Among them 9 were females and 10 males.

A. Session 1: surveillance of Civil Society: overview of trends and threats

8. In this session, participants discussed the historical context surrounding surveillance of society, the transformation of surveillance in the digital age, and the variety of ways surveillance can be conducted and impact human rights. Ultimately, participants agreed that surveillance tools create threats to human life, personal safety, cause reputational harm, and undermine public trust.

9. There was a consensus among participants that the overall discussion about human rights risks in relation to surveillance is quite broad. Participants noted that society has had

an intuition to search for new information, as manifested in the desire for "security" in the military context. This has grown to military-style counterterrorism strategies, the use of imitation profile accounts on platforms like Tinder and Facebook, facial recognition, mass surveillance, large scale targeted surveillance, and financial surveillance. It was agreed that each of these situations present unique challenges and threats to human rights.

10. Participants also noted that financial surveillance is a large-scale issue in multiple ways. One participant noted that certain entities and programs, like Google Pay, are closely related to the government. This raises concerns because surveillance in the banking industry allows for easier access to financial records of individuals and companies. This discussion also raised the issue of states providing non-governmental organisations (NGOs) or NGO members foreign funds in exchange for biometric data.

11. Participants noted that there are various actors, including those with political objectives, police officials, and those with public safety concerns, that have an interest in the information collected. Some participants suggested that private surveillance companies often function at the request of the government. They noted that the relationship between private surveillance providers and governments function as a revolving-door. This relationship raised several issues of concern: (i) What is the nature of the power dynamic between the companies, governments, and individuals; (ii) What is and what should be the relationship between transparency and privacy; and (iii) How do we define government entity?

12. The participants also agreed that national security or safety is often used as a justification for using private surveillance technology. One participant noted that the national security argument sometimes stretches into a good governance argument. Participants emphasized the concern with national security being loosely defined, particularly that the government is provided a lot of flexibility in justifying national security.

13. One concern raised was the difficulty of detecting the surveillance, yet people often "feel surveilled" creating a chilling effect on freedom of expression among civil society. Anonymity and encryption are often encouraged by human rights activists and civil society organizations. One participant noted that while these mechanisms are meant to protect individuals, it places the burden on the individual and not on the governments or private surveillance companies. One suggestion would be to determine what a more proactive approach looks like, including ideal legislation.

14. Participants also expressed concern that individuals defended by civil society organizations, like victims of targeted surveillance attacks, are not always aware of their rights or understand the harm. It can be difficult to advocate on behalf of civil society when the underlying issues are not always clear. There was one suggestion on increasing public education efforts.

15. Participants agreed that the legal framework regulating this technology is weak. One participant noted that at time the European Union haphazardly mimics the United States and this ultimately weakens surveillance efforts. Overall, countries are not following in their own laws. The suggestion was to make an effort to incentives governments to commit to the little framework they have. Additionally, larger companies like Microsoft have broadly used national laws in using technology like geotagging. Again, proactive legislation was suggested as a solution.

16. Participants also raised concerns with the hyper-masculinity surrounding the private surveillance industry. One participant suggested that larger colonial dimensions could be at play.

B. Session 2: the use of private surveillance tools

17. After having explored the multifaceted threats that the use of surveillance technologies poses in different parts of the world, the aim of this second session was to more specifically discuss the type of surveillance tools, identify if there are any trends in their use worldwide and better understand how companies develop and market them.

18. The first speaker expanded the scope of discussions by mentioning, beside targeted surveillance with malware, three other categories of surveillance tools: data mining tools, facial recognition, and marketing of vulnerabilities. Another participant drew attention to the issue of government use of open source intelligence to collect information that is publicly available, such as for example through CCTV surveillance cameras or social media surveillance. It was highlighted that political parties sometimes use this information without any form of consent.

19. Many participants stressed the importance for companies to endorse certain principles and norms in order to avoid adverse effects of their products on public freedoms. Microsoft was given as an example: it has recently adopted a set of principles and rules with respect to fairness, transparency, accountability, non-discrimination, consent and lawful surveillance in the development and deployment of their technologies. This seems to suggest that some companies are willing to commit. However, the question of how to make sure that these norms and principles will be endorsed was raised.

20. A participant observed as a recent trend that some internet companies have started to decline government's requests to collect and share information. Therefore, many States are trying to get rid of intermediaries in order to conduct their own surveillance. Some States even have the capacity and resources to develop their own tools. One participant insisted on the importance of States' disclosing which tools they have purchased and what type of information they are collecting. Another key issue mentioned is the problem of access to information, notably when some States consider that the information they are collecting is associated with national security threats. It has been noted that the private surveillance industry benefits from the opacity of security laws.

21. The increasing use of private surveillance by many governments throughout the world without any transparency or any sort of accountability is also associated with a serious problem of impunity. In Mexico for example, it was mentioned that there have been more than 20 cases of surveillance with malware thoroughly documented without any consequences to date. Many examples were given to illustrate that many transactions take place directly between governments.

22. Additionally, several participants agreed on the importance of working on the supply side through a stricter export control regime as the most effective way to prevent the use of technologies by authoritarian regimes.

23. A participant said that phishing tools and network surveillance are not being effectively addressed in the legal framework in Latin America, which makes strategic litigation more difficult. In general, States fail to consistently support requests for investigations. For example, Israel denied a request to compel NSO group to answer questions about their products and services being used in Mexico.

24. The relationship between governments and companies, not only during the development and enhancement of these technologies, but also once it has been transferred, has also been extensively discussed. The fact that former military and security personnel are using their expertise with companies and then contracted by governments is a source of concern. The issue of the customization of the surveillance tools by governments has also been put forward. Citizen Lab published a report last year on how certain tools are being marketed as customizable: for example, certain forensic software are being remodeled in improper ways.

25. Finally, the gendered nature of the digital surveillance industry and its masculine approach was further discussed. It is important to take into consideration the neocolonial dimensions of surveillance, particularly given that colonial patterns are being reproduced in the drafting of certain surveillance laws.

C. Session 3: State Responsibility and Targeted Surveillance

26. Participants discussed how to define state responsibility and what would be the most effective means of regulating private surveillance technologies. It was noted that the export

of the technology is not the only concern; governments that purchase such tools also pose a threat to freedom of expression and should hold responsibility as well.

27. The effect of legislation was questioned by multiple participants. Two distinct concerns were raised: (i) States have difficult implementing laws and (ii) companies can bypass State laws. One participant provided Hacking Team as an example where after they were exposed and regulated in Italy, they moved operations and continued operating in the same manner.

28. Participants generally noted that technology has played a role in developing surveillance tools, particularly over the last ten years. However, one participant observed that the sophistication of the targeted surveillance tools is usually low.

29. Participants focused discussion on what a legal framework should look like. A lot of problems were highlighted with the Wassenaar Arrangement including the fact it is non-binding, lacks transparency, and vaguely formulated. One participant noted that even members of the Wassenaar Arrangement fail to internalize the terms. Suggestions on improving the Wassenaar Arrangement included export controls criteria based on human rights concerns. One participant suggested that there is a lack of standards because there is no information sharing among States. Switzerland was used an example to demonstrate how a state can increase transparency by listing the licenses they approve and deny. However, this begged the question of whether more transparency is always better. It also raises concerns regarding capacity because the more items that the State controls, the more people will be needed to process. One participant expressed concerns regulating software or services like hacking under an export controls regime, since hacking software is already widely available and the service provided is intangible. A participant also stated that before regulating dual-use technology, we need to clearly define it.

30. The European Union has created ambitious goals to create firmer rules on surveillance technologies. However, one participant noted that there are internal clashes between different branches of government within the European Union and internally the EU has outdated frameworks. Participants agreed that the frameworks that exist are lacking an enforcement mechanism and do not cover all relevant technologies. However, there is a lot of information hidden in private-government relationships that hinder civil society's ability to close the gap. Some participants raised concerns that export-control debate is very westernized and fails to account for the acquisition and use of the technology by importing States.

31. Most participants agreed on the lack of enforcement of human rights standards when it comes to surveillance. Pressures coming from the private industry and IT sector, the lack of common standards for technologies and countries, broad and non-binding international soft law standards were all been mentioned as important issues.

32. The discussion raised important questions, including: (i) who are the targets of espionage, (ii) what are the ideal requirements for law enforcement, (iii) to what extent can the private surveillance industry be analyzed from a consumer rights perspective, and (iv) what is the ideal level of transparency in this industry.

D. Session 4: company responsibility: norms and enforcement

33. Almost all participants recognized the importance of the UN Guiding Principles on Business and Human Rights in establishing minimum baseline standards for corporates to respect human rights. Yet, most participants acknowledged that the industry is resistant to change and considered the legal framework for holding private surveillance industry accountable insufficient and unsatisfactory.

34. As possible further normative development, it was suggested that we look to other industries where there is an inherent state function or "service" of the state. One participant suggested analyzing private military contractors. One question here is whether surveillance would be categorized as a service of the state.

35. Additionally, a participant suggested we focus on technical standards and we view security and privacy as consumer needs. A participant raised the possibility of an ethics-based

framework that included training on human rights. The broader discussion on company normative development also noted the risk that increased normative development in the industry could lead governments to move towards weakening encryption standards.

36. One participant argued that technology embeds the values of those who make it. Therefore, there is a need for more awareness raising in engineering schools, to prepare students that will eventually be members of important standards setting bodies.

37. The lack of accountability associated with the use of surveillance was highlighted in relation to litigation surrounding FinFisher technology where an Ethiopian-born U.S. citizen and human rights activist living in the United States sued Ethiopia for monitoring his Skype calls over a four-month period. The litigation ultimately failed when the U.S. Court of Appeals for the District of Columbia Circuit concluded the wiretapping occurred abroad and foreign states are immune from suit in a U.S. court, unless an exception applies. One participant noted that accountability typically comes from customs regulation and without jurisdiction in the U.S. other avenues need to be explored. One concern in the U.S. is that the "harm" from the surveillance or monitoring is difficult to prove. A recommendation was made to look to trademark, unfair completion, and public agency arguments as alternatives to litigation in the United States.

38. The European Union General Data Protection Regulation (GDPR) was discussed as a regulation that can be looked to for industry standards as it includes "hard" language and is implemented by member states.

39. The discussion resulted in a variety of recommendations including the importance of having a competent authority creating and enforcing standards, annual and accurate reporting, and transparency. A multi-stakeholder approach is important. Key questions include: What are the companies we should be targeting here, and what is their due diligence?

E. Session 5: breakout brainstorming

40. After having spent a day exploring surveillance and the threats to civil society, participants broke out into smaller groups. Each group was assigned a specific question on how to hold the sale and deployment of private surveillance technologies accountable to human rights standards. Participants were asked to come with concrete outcomes and recommendations.

41. The first breakout group dealt with the issue of litigation in domestic or regional forums.

Key questions

42. What are the key challenges with public interest litigation against the sale or use of private surveillance technologies?

43. How might we develop strategies to overcome it?

44. The group identified (i) access to information, (ii) exceptions in data protection laws for intelligence services and (iii) compliance with court decisions to be some of the main challenges associated with public interest litigation against the sale or use of private surveillance technologies.

45. Several participants have pointed out the importance of using access to information laws and that this should apply to companies that collaborate with the government. To address the lack of knowledge of some judges, it has been suggested that they should be provided with adequate training. It was also pointed out that an independent investigation structure should be created in order to solve the issue of the lack of independence of investigative bodies. Several participants also stressed the importance in advocating for up-to-date laws, notably in connection with the issue of access to remedy. Finally, there was a general consensus within the group that joint litigation efforts should be improved, given that in most cases multiple jurisdictions are involved.

46. The second breakout group tackled the issue of corporate responsibilities.

Key questions

47. What should a private surveillance company's responsibility to respect end-users' rights encompass?

48. What are elements of a persuasive advocacy strategy vis-a-vis these companies?

49. The issues of digital security vulnerabilities, the relationship between the companies that develop surveillance tools and governments that buy these technologies and applicable normative frameworks were at the core of this discussion.

50. Several participants of this group underlined the limitations and constraints associated with the UN Guiding Principles on Business and Human Rights and called for the development of additional norms to ensure the accountability of the private sector in this field. The Montreux Document on Private Military and Security Companies was discussed as an example on how to provide incentives for States to ensure corporate compliance with international human rights standards. Participants argued that similar codes of conduct or standards could be adopted and applied to the issue of private surveillance.

51. Given the potential risk of misuse and adverse impact on human rights, the importance for companies to contract directly and only with those who can legally use their product and services was underlined. Furthermore, companies should resist demands from governments to make products less safe and should instead invest in the safety of their products.

52. The option of establishing a multi-stakeholder review entity has also been put forward by one of the participants. Some participants stressed the need for companies, as part of their due diligence obligations, to cooperate with investigations into alleged abuses.

53. Other recommendations include: identifying and engaging public facing companies based on the importance of their public image and reputation, persuading governments that these tools may eventually be used against them, and encouraging the development of extraterritorial norms.

54. The third breakout group focuses on controls on transfer, international and domestic.

Key questions

55. What are the key improvements necessary in the international regime governing transfer of surveillance technology?

56. Is it even subject to such control?

57. The absence of enforcement mechanism within the Wassenaar Agreement has been identified as one of the biggest challenge associated with the international regime control. Hence, several participants proposed the creation of a report mechanism within the agreement.

58. Many participants emphasized the need for greater transparency from States on the list of items that are being exported and under which criterion the export is authorized. The group agreed that civil society organizations should be able to provide their inputs on export controls. It was also said that exporting countries should only allow licenses for technologies to be used in countries with an appropriate level of human rights commitment. One participant also stressed the importance of developing a mechanism outside of Wassenaar that would foster collaboration and information sharing for the purposes of strategic litigation.

59. Issues of due diligence also generated some discussion. Several participants agreed on the importance to adopt more clear and concrete rules following the UN Guiding Principles.

60. The group ended its presentation addressing two questions to the audience:

61. What is the role for international sanctions in cases where the importing State lacks the requisite commitments to human rights?

62. What incentives can be provided to bring more countries into compliance with export control regimes (at both local and international levels)?

63. The fourth group worked on the issue of international normative development.

Key questions

64. How should international and regional mechanisms support and encourage the development of rights-oriented standards and norms governing the private surveillance industry and the use of these tools?

65. What is the role of regional bodies, such as the OECD, the European Commission and the Inter-American Commission on Human Rights?

66. What is the role of standard-setting organizations (such as the Internet Engineering Task Force or Institute of Electrical and Electronics Engineers) and other technical bodies (such as the International Telecommunications Union)?

67. The participants discussed potential ways to create "best practices" for the private surveillance industry. There was no general consensus on the overall mechanism to establish best practices. Participants noted that in addition to industry self-regulation, looking at the World Wide Web Consortium (W3C) and the Organisation for Economic Co-operation and Development (OECD) could be helpful. The OECD may be particularly useful for developing relevant norms concerning the financial industry.

68. One participant mentioned that governments may create "action plans" on governing private surveillance tools. Participants deliberated on how to identify the desired principles of an action plan and whether or not action plans would be useful. Ultimately, participants agreed that whatever mechanism is used, they should include, at a minimum, strategies for mitigating surveillance-related human rights abuses. But there was no consensus on whether action plans were the most effective way to encourage rights-oriented standards.

69. Other suggestions for normative development included: improving or developing protocols for e-mail communication from States and companies, in order to better distinguish genuine communications from those that are phishing e-mails in disguise. Governments and companies may also consider ways to educate users on avoiding malicious links and suspicious requests. In relation to company responsibility, the participants discussed using human rights impact assessments to increase transparency and awareness. Concerns were raised about the accuracy of such assessments, how such information would be framed, and what companies would overlook. One participant suggested that an independent impact assessment could potentially increase transparency and alleviate concerns.