United Nations A/HRC/41/35

General Assembly

Distr.: General
28 May 2019

Original: English

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

Surveillance and human rights

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

Summary

Surveillance of individuals – often journalists, activists, opposition figures, critics and others exercising their right to freedom of expression – has been shown to lead to arbitrary detention, sometimes to torture and possibly to extrajudicial killings. Such surveillance has thrived amid weak controls on exports and transfers of technology to Governments with well-known policies of repression. In the present report, the Special Rapporteur begins by identifying the problem of targeted surveillance seen from the obligations that human rights law imposes on States and the related responsibilities of companies. He then proposes a legal and policy framework for regulation, accountability and transparency within the private surveillance industry. He concludes with a call for tighter regulation of surveillance exports and restrictions on their use, as well as a call for an immediate moratorium on the global sale and transfer of the tools of the private surveillance industry until rigorous human rights safeguards are put in place to regulate such practices and guarantee that Governments and non-State actors use the tools in legitimate ways.

* The present report was submitted after the deadline in order to reflect the most recent information.

GE.19-08652(E)
1908652

Contents

I. Introduction

1. The General Assembly has condemned unlawful or arbitrary surveillance and interception of communications as "highly intrusive acts" that interfere with fundamental human rights (see General Assembly resolutions 68/167 and 71/199). However, unlawful surveillance continues without evident constraint. Submissions for the present report detailed case after case of Governments using surveillance software developed, marketed and supported by private companies. Surveillance of specific individuals – often journalists, activists, opposition figures, critics and others exercising their right to freedom of expression – has been shown to lead to arbitrary detention, sometimes to torture and possibly to extrajudicial killings. Such surveillance has thrived amid weak controls on technology transfers to Governments with well-known policies of repression. The market is shrouded in secrecy; indeed, our knowledge of the problem exists mainly because of the digital-forensic work of non-governmental researchers and tenacious reporting by civil society organizations and the media.

2. The problem is serious enough that the Special Rapporteur concludes the present report with a call not merely for tighter regulation of surveillance exports and restrictions on their use, but for an immediate moratorium on the global sale and transfer of the tools of the private surveillance industry until rigorous human rights safeguards are put in place to regulate such practices and guarantee that Governments and non-State actors use the tools in legitimate ways.

3. The Special Rapporteur proposes a legal and policy framework for regulation, transparency and accountability within the private surveillance industry. He begins by identifying the problem, emphasizing its focus on targeted surveillance, leaving aside the issue of bulk interception, collection and retention of private data (often referred to as "mass surveillance"). He then highlights the obligations human rights law imposes on States and the related responsibilities of companies. In part IV, he proposes a framework to improve on existing laws and policies by incorporating protection of the rights to freedom of opinion and expression, based on existing international human rights law. He concludes by making recommendations for key actors.

4. Preparation of the present report benefited from 11 submissions by States and 33 by civil society. The Office of the High Commissioner for Human Rights organized a two-day consultation with experts in Bangkok in December 2018. The submissions and the talks held during the consultation are summarized in an addendum to the present report.[1]

II. Governments and the private surveillance industry

5. We live in an age of readily available, easy to abuse and difficult to detect tools of digital surveillance. In his groundbreaking surveillance report in 2013, the previous mandate holder, Frank La Rue, noted that weak regulatory environments had provided fertile ground for arbitrary and unlawful infringements of the rights to privacy and freedom of opinion and expression (A/HRC/23/40, para. 3). In his inaugural report the following year on privacy in the digital age, the High Commissioner for Human Rights concluded that practices in many States involved a lack of adequate national legislation and/or enforcement, weak procedural safeguards and ineffective oversight, all of which had contributed to a lack of accountability for unlawful digital surveillance (A/HRC/27/37, para. 47).

6. Some States develop targeted surveillance tools within their own agencies and departments, others repurpose existing "off the shelf" crimeware products and others may

[1] I especially want to thank Amos Toh, Desiree Murray, Cristina Butoiu, Matthew Marcoly and Kyoolee Park of the International Justice Clinic, University of California, Irvine School of Law, for their assistance in the preparation of the present report and its addendum.

purchase sophisticated commercial spyware on the international surveillance market.[2] In the present report, the Special Rapporteur is most concerned with the last category of tools. Digital surveillance is no longer the preserve of countries that enjoy the resources to conduct mass and targeted surveillance based on in-house tools. Private industry has stepped in, unsupervised and with something close to impunity. According to Privacy International, in 2016 there were well over five hundred companies developing, marketing and selling such products to government purchasers.[3]

Types of surveillance considered in the present report

7. In the present report, the Special Rapporteur is principally concerned with technologies that enable an actor to gain surreptitious access to the digital communications, work product, browsing data, research, location history and online and offline activities of individuals. Key targeted surveillance technologies and practices are described below.

Computer interference

8. Surveillance technologies may enable intruders to gain access to an individual's computer or network. The range of such interference is substantial.[4] For instance, in 2017, an appeals court in the United States of America heard the case of foreign State-sponsored surveillance on United States soil.[5] The case concerned a citizen of the United States born in Ethiopia and living in the state of Maryland who had been providing technical assistance to members of the Ethiopian diaspora community. A document originally sent to an activist by agents of the Government of Ethiopia infected his computer with an intrusive form of malware, a program called FinSpy marketed by a German-British company, Gamma Group.[6] FinSpy allegedly recorded the man's and his family's Internet video calls, emails and other communications, including by logging his keyboard strokes, sending the data back to servers based in Ethiopia.[7]

Mobile device hacking

9. Private surveillance products also offer the capability of hacking directly into mobile devices. The NSO Group's Pegasus spyware is a paradigmatic example and its alleged use in Mexico is instructive. Beginning in 2015, numerous individuals reporting on corruption and the drug trade received text messages or links on their mobile devices, some from seemingly legitimate sources suggesting detailed knowledge of the targets. Journalists, politicians, United Nations investigators, human rights advocates and others received these texts. A Canadian research and advocacy organization, Citizen Lab, found that the links infected the devices with the Pegasus spyware, allowing the targets to be monitored remotely. Citizen Lab has identified Pegasus software being used as a surveillance tool targeting individuals in 45 countries, including Bahrain, Saudi Arabia, Togo, the United Kingdom of Great Britain and Northern Ireland and the United States.[8]

Social engineering

10. Many of the technologies described above are accompanied by strategies to lure a target into unwittingly downloading malware on their devices. For example, emails

[2] Citizen Lab, *Communities @ Risk: Targeted Digital Threats Against Civil Society* (Toronto, Monk School of Global Affairs, University of Toronto, 2014), Executive Summary, pp. 8–11.

[3] Privacy International submission, p. 1.

[4] See, e.g., Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto, Signal, 2013), pp. 186–190.

[5] *Doe v. Federal Democratic Republic of Ethiopia*, 851 F.3d 7 (D.C. Cir. 2017).

[6] For FinSpy's promotional material, see Wikileaks, "The spy files: remote monitoring and infection solutions: FINSPY".

[7] For details of the allegations, see the *first amended complaint, Doe v. Federal Democratic Republic of Ethiopia* (18 July 2014).

[8] See Bill Marczak and others, "Hide and seek: tracking NSO Group's Pegasus spyware to operations in 45 countries", Citizen Lab, 18 September 2018.

containing malicious links either impersonate the target's contacts or trick the target into believing that they are clicking on a benign link related to their work, advocacy or personal affairs. For example, a WhatsApp message linked by researchers to Pegasus spyware was sent to an Amnesty International staff member urging him to cover a protest, including a link that it claimed would lead to additional information.[9] Clicking on the link would likely have downloaded the spyware on his device.

Network surveillance

11. Some technologies work on a network to enable targeted surveillance. For instance, the Russian System for Operative Investigative Activities involves the installation of a device on telecommunications networks that enables interception of communications. The system is privately manufactured and marketed and is widely used in the Russian Federation and further afield in Central Asia. For example, the company Protei manufactures equipment that ensures that the system's technologies, such as eavesdropping and Internet interception tools, work in countries like Uzbekistan and Kazakhstan.[10]

Facial and affect recognition

12. Facial recognition technology seeks to capture and detect the facial characteristics of a person, potentially profiling individuals based on their ethnicity, race, national origin, gender and other characteristics, which are often the basis for unlawful discrimination.[11] Affect recognition seeks to infer a person's feelings, emotions or intentions from facial expressions, based on highly questionable classification systems.[12] Perhaps no other environment demonstrates the comprehensive intrusiveness of these technologies better than China. Credible reporting suggests that the Government of China, using a combination of facial recognition technology and surveillance cameras throughout the country, "looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review".[13] Much of the technology deployed by the Government appears to be produced domestically, by both State-owned and private enterprises.[14]

International Mobile Subscriber Identity catchers (Stingray)

13. International Mobile Subscriber Identity catchers mimic nearby cell towers to intercept communications and location data being transmitted by personal communication devices. Such catchers are widely used around the world, often by law enforcement and intelligence agencies. A private company in the United Kingdom allegedly sold such catchers and other spyware to the Philippines, and many fear that these tools were used to track and monitor drug users in the Government's widely criticized war on drugs.[15]

Deep Packet Inspection

14. Deep Packet Inspection enables the monitoring, analysis and redirection of traffic passing through communications and Internet networks. It can also be used to redirect users to sites infected with malware and block them from accessing certain websites. Such devices were reportedly installed on Türk Telekom's network, and deployed to redirect

[9] See Bill Marczak, John Scott-Railton and Ron Deibert, "NSO Group infrastructure linked to targeting of Amnesty International and Saudi dissident", Citizen Lab, 31 July 2018.

[10] Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York, PublicAffairs, 2015), pp. 190–191.

[11] See, e.g., Internet Lab submission, p. 6; and Center for Internet and Society submission, p. 12.

[12] AI Now Institute, *AI Now Report 2018* (New York, New York University, 2018), pp. 13–14.

[13] See Paul Mozur, "One month, 500,000 face scans: how China is using A.I. to profile a minority", *New York Times*, 14 April 2019.

[14] Human Rights in China submission, pp. 2–3. See also A/HRC/39/29, para. 14.

[15] See Sofia Tomacruz, "You think your data, communication devices are safe? Think again", Rappler, 17 March 2018.

users in Turkey and the Syrian Arab Republic to download spyware when they attempted to download legitimate software applications.[16]

Public-private collaboration

15. Governments and the private sector are close collaborators in the market for digital surveillance tools. Governments have requirements that their own departments and agencies may be unable to satisfy. Private companies have the incentives, the expertise and the resources to meet those needs. They meet at global and regional trade shows designed, like dating services, to bring them together.[17] From there, they determine whether they are a match. Whether companies carry out any kind of due diligence to evaluate the human rights record of purchasers is unknown.

16. The seller's intentions may be legitimate. It may be that companies genuinely intend their products to be deployed for "lawful interception" by authorized public authorities against legitimate targets, with the authorization of judicial or other independent actors. However, this cannot be known for certain because every aspect of such collaboration – from due diligence and sales to end-user support – typically operates with limited oversight and transparency. In fact, nearly all the publicly available information about the private surveillance industry has been gathered during the forensic work carried out by non-governmental and academic institutions, such as Citizen Lab, and investigative reporting.[18]

17. The operation of the so-called "vulnerabilities market" is especially murky. Governments and private actors are known to purchase security vulnerabilities in commonly available software from security researchers, to be utilized as "zero-day exploits" for the purpose of gaining access to individual communications and devices.[19] So long as they remain undisclosed to the device or software manufacturer, vulnerabilities may serve as an entry point for surveillance. When Governments and companies fail to disclose such vulnerabilities, they put at risk the security of end users, including government and private sector clients that store sensitive financial, health, employment or law enforcement data in commercially developed databases. To date, there has been no agreement as to whether Governments and companies have a responsibility to share their knowledge of vulnerabilities, and the sale of such vulnerabilities is unregulated. In fact, not only has the situation facilitated the development of a valuable market in vulnerabilities, it has led many Governments and companies to guard their knowledge of vulnerabilities jealously in the hope of using them for offensive purposes.[20]

18. It is also evident that public-private collaboration does not end at the point of sale and transfer of product. Leaked documents have demonstrated that private surveillance companies provide after-sales support. For example, in 2014, FinFisher reportedly entered into "annual support contract[s]" with government clients to provide technical upgrades and updates to the products and other forms of customer support.[21] They also conduct training

[16] See Bill Marczak and others, "Bad traffic: Sandvine's PacketLogic devices used to deploy government spyware in Turkey and redirect Egyptian users to affiliate ads?", Citizen Lab, 9 March 2018.

[17] See, e.g., www.issworldtraining.com; and Patrick Howell O'Neill, "ISS World: the traveling spyware roadshow for dictatorships and democracies", Cyberscoop, 20 June 2017.

[18] The story of private surveillance is also a story of the critical importance of free and independent research and media. Such investigations have also put the investigators at risk of surveillance. See, e.g., Raphael Satter, "Undercover agents target cybersecurity watchdog", Associated Press, 26 January 2019.

[19] See Privacy International, "Exploiting privacy: surveillance companies pushing zero-day exploits", 7 February 2018.

[20] See the discussion in Sarah McKune submission, pp. 2–4; Centre for European Policy Studies, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges* (Brussels, June 2018); and Sven Herpig and Ari Schwartz, "The future of vulnerabilities equities processes around the world", Lawfare, 4 January 2019.

[21] See Privacy International, "Six things we know from the latest FinFisher documents", 15 August 2014.

on how to optimize their malware to compromise the digital communications, computer devices and Wi-Fi networks of surveillance targets.[22]

19. Just as the companies and the purchasers are tightly connected, so too are the companies and Governments in the countries in which they are based. Some of the companies have powerful voices in their countries' export control regimes and have undermined efforts to strengthen them. For instance, in 2016, credible allegations suggested that, as a result of pressure from industry lobbyists, certain forms of surveillance technology had been removed from a proposed list of additions to the European Union list of dual-use goods and technologies subject to export controls.[23] During recent negotiations on the European Union export control regime, business interests were alleged to have influenced the decision to significantly curtail the inclusion of human rights safeguards in proposed regulatory changes, despite broad agreement on their adoption in the European Parliament.[24]

20. It has also been indicated in recent reports that many individuals with intelligence and law enforcement expertise and experience move between government and private sector positions. This revolving door may enable former government experts to support private actors whose tools may be used to violate human rights.[25] In a 2019 report, Reuters revealed that several former United States National Security Agency employees moved to a private company to support United Arab Emirates signals intelligence programmes under the code-name "Project Raven".[26] The employees in question allegedly deployed their expertise to surveil political opponents of the authorities of the United Arab Emirates and target citizens of the United States. Government regulation of the "revolving door" with respect to the private surveillance industry appears at best weak and likely does not exist in many, if not most, legal systems.

III. Legal framework

A. State obligations

21. Targets of surveillance suffer interference with their rights to privacy and freedom of opinion and expression whether the effort to monitor is successful or not.[27] The target need have no knowledge of the attempted or successful intrusion for the interference with their right to privacy to be complete. Indeed, Governments generally seek tools that intrude without the knowledge of the target. However, it is critical to see such interference as part of an overall effort to impose consequences on the target. If conducted for unlawful purposes, the attempt at surveillance – and the successful operation – may be used in an effort to silence dissent, sanction criticism or punish independent reporting (and sources for that reporting).[28] The sanctions may not be applied to the targets but to their networks of contacts. In environments subject to rampant illicit surveillance, the targeted communities know of or suspect such attempts at surveillance, which in turn shapes and restricts their capacity to exercise the rights to freedom of expression, association, religious belief, culture

[22] Ibid.

[23] See Reporters Without Borders, "International regulations: broken or blocked by lobbies", 14 March 2017.

[24] See Daniel Moßbrucker, "Surveillance exports: how EU Member States are compromising new human rights standards", netzpolitik.org, 29 October 2018.

[25] See Privacy International, "Switching hats: why South Africa's surveillance industry needs scrutiny", 14 December 2016; and Alex Kane, "How Israel became a hub for surveillance technology", The Intercept, 17 October 2016.

[26] See Christopher Bing and Joel Schectman, "Inside the UAE's secret hacking team of American mercenaries", Reuters, 30 January 2019; Robert Chesney, "Project Raven: what happens when U.S. personnel serve a foreign intelligence agency", Lawfare, 11 February 2019; and Sarah McKune submission, pp. 7–8.

[27] Global Justice Clinic, New York University School of Law, submission, p. 6.

[28] See Human Rights Foundation submission.

and so forth. In short, interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression.

22. It is not necessary to duplicate the extensive human rights reporting that has already been conducted by previous Special Rapporteurs, other mandate holders, the High Commissioner, the Human Rights Council, the Human Rights Committee and others, in which they highlighted the following key features of the human rights legal framework that protects against targeted surveillance.

23. First, the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights protect everyone's rights to privacy, opinion and expression. Article 19 of both instruments protects everyone's right to hold opinions without interference and to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media. Article 17 (1) of the Covenant, echoing article 12 of the Declaration, provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence".

24. Privacy and expression are intertwined in the digital age, with online privacy serving as a gateway to secure exercise of the freedom of opinion and expression (A/HRC/29/32; and A/HRC/23/40, para. 24). Article 17 permits interference with the right to privacy only where it is "authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant", is in pursuit of "a legitimate aim" and "meet[s] the tests of necessity and proportionality" (A/69/397, para. 30). Article 19 articulates a three-part test requiring that restrictions be provided by law and be necessary to protect the rights or reputations of others, national security or public order, or public health or morals.[29] The Human Rights Committee has emphasized that these principles, at a minimum, mean the following:

(a) Provided by law/legality: any restriction must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. Any restriction may not be unduly vague or overbroad such that it could confer unfettered discretion on officials;[30]

(b) Necessity and proportionality: the State has the burden of proving a direct and immediate connection between the expression and the threat and that the restriction it seeks to impose is the least intrusive instrument among those that might achieve the same protective function;[31]

(c) Legitimacy: article 19 (3) imposes specific limits on the interests justifying restrictions. While it is common for States to seek to justify restrictions, especially targeted surveillance, on the bases of national security, the Special Rapporteur has found that this rationale should be limited in application to situations in which the interest of the whole nation is at stake, which would thereby exclude restrictions in the sole interest of a Government, regime or power group (A/71/373, para. 18).

25. The Human Rights Committee put these principles into practice in its 2017 concluding observations on the sixth periodic report of Italy under the International Covenant on Civil and Political Rights (CCPR/C/ITA/CO/6, para. 36). It determined that the right to privacy required that robust, independent oversight systems were in place regarding surveillance, interception and hacking, including by ensuring that the judiciary was involved in the authorization of such measures, in all cases, and by affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they had been placed under surveillance or that their data had been hacked (ibid., para. 37). The General Assembly, in its resolution 73/179, echoed these principles, noting that surveillance of digital communications must be consistent with international

[29] Detailed explication of the three-part test under article 19 may be found in Human Rights Committee, general comment No. 34 (2011) on the freedoms of opinion and expression, paras. 5–9 and 22–36; and A/HRC/38/35.

[30] General comment No. 34, para. 25.

[31] Ibid., paras. 34–35.

human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory.

26. While these principles apply in all cases of targeted surveillance, they have particular force when expression in the public interest is implicated. Targeted surveillance creates incentives for self-censorship and directly undermines the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information (A/HRC/38/35/Add.2, para. 53). The Committee has emphasized that restrictions may never be invoked as a justification for the muzzling of any advocacy of multiparty democracy, democratic tenets and human rights.[32] Attacks on a person because of the exercise of his or her right to freedom of expression may not be justified by article 19 (3).[33] The Committee further singled out the importance of protecting journalists and persons who engaged in the gathering and analysis of information on the human rights situation and who published human rights-related reports, including judges and lawyers.[34] These protections extend to the confidentiality of sources, which international and regional human rights mechanisms (in the African, European and inter-American systems) have emphasized should be protected under law (A/70/361, para. 5).

27. In addition to the primary obligations not to interfere with privacy or restrict expression, States also have duties to protect individuals against third-party interference. Article 2 of the International Covenant on Civil and Political Rights, reflecting the primary duties of States, imposes an obligation to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the Covenant.[35] Article 17 (2) of the Covenant provides that everyone has the right to the protection of the law against unlawful interference with his or her privacy. However, it is not clear that States generally afford affirmative legal protections against targeted surveillance. This is certainly true of transnational surveillance, even when committed by foreign entities against one's own citizens.[36] In one instance concerning the allegations of targeted surveillance in Mexico, the Special Rapporteur for freedom of expression in the Inter-American Commission on Human Rights and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression conducted a joint mission to the country in which they raised the issue of the Government's use of the Pegasus spyware. They urged the Government to allow an independent investigation of the allegations that the spyware was deployed against journalists (A/HRC/38/35/Add.2, paras. 52–55). To date, the efforts to investigate the allegations have not clarified the situation, despite the orders of the National Institute for Transparency, Access to Information and Personal Data Protection of Mexico that the Government reveal the nature of its contracts to obtain Pegasus.[37]

28. It is clear from the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework adopted by the Human Rights Council in 2011, that a State's duty to protect includes a duty to take appropriate steps to prevent, investigate, punish and redress human rights abuse by third parties (A/HRC/17/31). In the Guiding Principles, States are urged to exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, business enterprises to provide services that may have an impact on the enjoyment of human rights (ibid., p. 10).

[32] General comment No. 34, para. 23.

[33] Ibid.

[34] Ibid.

[35] See also Human Rights Committee, general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the Covenant. Note that under general comment No. 31, article 17 on privacy is specifically included as an example of an article in which there are positive obligations on States parties to address the activities of private persons or entities.

[36] See Nate Cardozo, "D.C. circuit court issues dangerous decision for cybersecurity: Ethiopia is free to spy on Americans in their own homes", Electronic Frontier Foundation, 14 March 2017.

[37] See Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Fiscalía general de la República tiene oportunidad histórica para acabar con la impunidad en caso Pegasus: Salas Suárez", 27 March 2019; and Juan Arvizu, "Ordena Inai a PGR abrir contrato de compra de Pegasus", *El Universal*, 17 April 2018.

B. Corporate responsibility

29. Because the companies in the private surveillance industry operate under a cloak of secrecy, the public lacks any information about the way in which they may – if at all – consider the human rights impacts of their products. Given the nature of the industry and the widespread use of its products for purposes that are inconsistent with international human rights law, it is difficult to imagine that they do in fact take such impacts into account. Put another way: given the broad public knowledge of the repression practised by many of their clients, the companies cannot seriously claim to lack insight into the repressive uses of their tools.

30. The Guiding Principles provide a framework for assessing whether surveillance companies respect the rights of those affected by their products and services. In particular, there is an emphasis in the Guiding Principles on policy commitments to respect human rights; due diligence processes to identify, prevent, mitigate and account for human rights impacts; consultation with affected groups; ongoing evaluation of the effectiveness of human rights policies; and effective grievance mechanisms for affected rights holders (A/HRC/17/31, paras. 15–25).

31. By every measure, the companies would appear to fail to meet even these minimum baselines. The few companies that have published their customer policies gesture vaguely at the need to respect human rights. Hacking Team, for instance, states that it reviews "potential customers before a sale to determine whether or not there is objective evidence or credible concerns that Hacking Team technology provided to the customer will be used to facilitate human rights violations", but does not explain what it does with such information, or even identify which human rights its technologies might implicate.[38] The NSO Group claims to operate in accordance with a Business Ethics Committee, "which includes outside experts from various disciplines, including law and foreign relations", and suggests that it may cancel work if its products are put to "improper use".[39] On its website, it also states that it will "investigate any credible allegation of product misuse", but there is no indication of whether that includes human rights violations.[40]

32. In short, companies have not disclosed instances of meaningful action, such as putting in place due diligence processes that identify and avoid causing or contributing to adverse human rights impacts through their own activities and that prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships (A/HRC/17/31, annex, principle 13) There is, for example, no public information suggesting that human rights assessments are a routine component of due diligence during sales, that companies give decisive weight to these assessments and that these assessments continue throughout the life cycle of the product and any contract for after-sales support. Indeed, mounting evidence of the industry's central role in facilitating gross human rights abuses, coupled with its steadfast refusal to explain its safeguards, makes it difficult to avoid the conclusion that such self-regulation lacks substance.

33. The guidance of the European Commission on implementing the Guiding Principles in the information and communications technology sector highlights the importance of "human rights by design".[41] The extraordinary risk of the misuse of surveillance products means that companies should anticipate the illicit use of their software and begin engineering solutions for the inevitable negative impacts. In a promising move, the

[38] Hacking Team, Customer Policy.

[39] See NSO statement of 17 September 2018. Available at https://citizenlab.ca/wp-content/uploads/2018/09/NSO-Statement-17-September-2018.pdf. As a Citizen Lab puts it, "NSO's statements about a Business Ethics Committee recall the example of Hacking Team's 'outside panel of technical experts and legal advisors … that reviews potential sales.' This 'outside panel' appears to have been a single law firm, whose recommendations Hacking Team did not always follow" (Marczak and others, "Hide and seek").

[40] See www.nsogroup.com/about.

[41] See European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (Luxembourg, 2013).

Government of the United Kingdom, in partnership with a technology industry association, produced a set of guidelines for the cybersecurity industry in which they stress the importance of preventing and mitigating human rights risks "through appropriate design modification" at the earliest stages of product development.

C. International and domestic export control

34. Export controls are an important element of the effort to reduce the risks caused by the private surveillance industry and the repressive use of its tools. However, their effectiveness is limited. First, the relevant international export control regime – the non-binding Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, in which 42 States participate – is tailored to reduce threats to regional and international security. While that is a laudable and necessary objective, the framework is ill-suited to addressing the threats that targeted surveillance pose to human rights; indeed, it lacks guidelines or enforcement measures that would directly address human rights violations caused by surveillance tools. Second, the focus on exports is an imperfect proxy for addressing the central problem: the use of such technologies to target lawful expression, dissent, reporting and other examples of the exercise of human rights.

35. The Wassenaar Arrangement nevertheless promotes important goals of "transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies". Participating States are expected to apply export controls to all items on the list of dual-use goods and technologies.[42] As such, the Wassenaar Arrangement has been (or should be) internalized in domestic law and policy by participating and non-participating States; unfortunately, there is no enforcement mechanism to ensure its translation into domestic law or its implementation by the relevant domestic agencies.

36. In 2013, the participating States added items related to "intrusion software" and Internet Protocol network communications surveillance systems to the list of dual-use technologies. According to the list, intrusion software is "'software' specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures'", which either extracts data from a computer or network device or modifies the "standard execution path" of a program to allow "the execution of externally provided instructions".[43]

37. The detailed reports of surveillance-related abuses demonstrate that the export control regime centred on the Wassenaar Arrangement has not meaningfully limited the spread of surveillance technologies and their use for repressive purposes. A stalled effort by European parliamentarians to strengthen the human rights protections in European export laws and policies demonstrated the challenges of reform. Their effort explicitly called for expansion of the list of dual-use items and catch-all controls, and the consideration of "respect for human rights in the country of final destination" of the surveillance technologies.[44] In January 2018, this proposal went through first reading in the European Parliament, originally gathering support to implement stronger controls on exports of dual-use technology.[45] However, the proposal has since received criticism from at least nine member States, which argued for weaker human rights protections.[46] The future of the legislation is now unclear.[47]

[42] See Wassenaar Arrangement, "List of dual-use goods and technologies and munitions list".

[43] Ibid., p. 221.

[44] See European Commission, "Proposal for a regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)", 28 September 2016; and Lucie Krahulcova, "The European Parliament is fighting to strengthen the rules for surveillance trade", Access Now, 8 December 2017.

[45] For an overview of the legislative history of the aforementioned proposed regulation, see EUR-Lex, Doc. 52016PC0616.

[46] Delegations of Cyprus, Czechia, Estonia, Finland, Ireland, Italy, Poland, Sweden and the United Kingdom, "For adoption of an improved EU Export Control Regulation 428/2009 and for cyber-surveillance controls promoting human rights and international humanitarian law globally", WK

38. At the domestic level, the enforcement of export controls varies, even among participating States in the Wassenaar Arrangement. For example, the United States has yet to adopt the 2013 additions of items related to intrusion software and Internet protocol network communications surveillance systems.[48] However, the United States Commerce Department is conducting a broad review of the current framework and has been commissioned to establish an inter-agency process for setting new controls for both "emerging" and "foundational" technologies under the Export Control Reform Act of 2018.[49] Israel, a non-participating State, has adopted export controls on dual-use items regulated under the Wassenaar Arrangement, but its enforcement of these controls is shrouded in secrecy.[50]

D. Absence of remedies for targeted surveillance

39. As part of a State's duty to respect and ensure enjoyment of human rights, article 2 (3) (a) of the International Covenant on Civil and Political Rights imposes an obligation to provide victims of violations with access to an effective remedy. It is specified in article 2 (3) (b) that claims of such violations must be determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State. The Human Rights Committee has stressed that law enforcement and prosecutorial authorities should investigate allegations of violations promptly, thoroughly and effectively through independent and impartial bodies.[51] The duty to provide effective remedies also entails an obligation to protect individuals from acts by private sector entities that cause infringements, by exercising due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities.[52]

40. Victims of targeted surveillance have had little success in their efforts to obtain recognition of the harm suffered, let alone remedies for such harm. This is so even though, as explained by both the European Court of Human Rights and the High Commissioner for Human Rights, the mere threat of surveillance, even when secret, coupled with the lack of remedy, can constitute an interference with the right to privacy.[53]

41. Litigation as a course of action to seek remedy against private surveillance companies that manufacture and sell tools and Governments that deploy them is uncertain. The lack of causes of action and remedies raises serious concerns about the likelihood of holding companies accountable for human rights violations. Alleged victims have commenced litigation or formal complaints against private surveillance companies or Governments in at least eight countries.[54] However, the barriers to successful litigation and formal complaints are significant, including the lack of judicial oversight, remedies, causes of action, enforcement and data preservation.

42. In some cases, civil society organizations have requested that Governments investigate unlawful surveillance, but these requests are frequently rejected. In the United Kingdom, Privacy International made a criminal complaint against Gamma Group to the National Crime Agency, arguing that the company had violated multiple domestic laws when its subsidiary, FinFisher, sold surveillance technologies and provided assistance to the

5755/2018 INIT (15 May 2018); and Access Now, "EU: States push to relax rules on exporting surveillance technology to human rights abusers", 11 June 2018.

47 See Catherine Stupp, "Nine countries united against EU export controls on surveillance software", Euractiv, 11 June 2018; and Moßbrucker, "Surveillance exports".

48 Privacy International submission, p. 5.

49 John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law No 115–232 (2018).

50 See "Israel-U.S. export controls", export.gov, 20 July 2018. See also para. 43 below.

51 General comment No. 31, para. 15.

52 Ibid., para. 8.

53 European Court of Human Rights, *Roman Zakharov v. Russia* (application No. 47143/06), judgment of 4 December 2015, para. 171; and A/HRC/27/37, para. 20.

54 See Siena Anstis, "Litigation and other formal complaints concerning targeted digital surveillance and the digital surveillance industry", Citizen Lab, 12 December 2018.

Government of Bahrain.[55] The European Centre for Constitutional and Human Rights and Privacy International also filed a criminal complaint in Munich, Germany, calling for an investigation into the company, but the public prosecution authorities refused the request.[56] Even when States open investigations to determine whether government surveillance violated human rights norms or State laws, the investigations can be arbitrary or disorganized.

43. Alternatives to litigation, providing for remedies consistent with international human rights law, appear unavailable. For instance, after an Amnesty International staff member was the target of a suspicious WhatsApp message allegedly linked to Pegasus, the organization wrote to the Ministry of Defence of Israel asking that the NSO Group's export licence be revoked.[57] The country's Defence Export Control Agency sent a letter in response, stating that it does not provide information on its policies on granting export licences or any information on the actual licences themselves.[58] The Agency did not confirm or deny the existence of the export licence, but did note that "that export licences issued by the Israeli [Ministry of Defence] to NSO Group in relation to its government clients are consistent with international obligations".[59] The lack of regional and international pressure and non-disclosure policies justified on the basis of national security prove to be significant barriers.

44. Privacy International has also filed complaints with the Organization for Economic Cooperation and Development (OECD) National Contact Points for Germany and the United Kingdom against Gamma and Trovicor for their alleged roles in the targeted surveillance of political opponents by the Government of Bahrain.[60] The complaint against Trovicor asked the National Contact Point for Germany to "ascertain whether the company breached the OECD Guidelines for Multinational Enterprises by exporting surveillance products to Bahrain, where the authorities use such products in human rights abuses, including the arrest, detention and torture of political opponents and dissidents".[61] However, the National Contact Point rejected the complaint on the basis that the evidence of Trovicor's presence in Bahrain was not sufficient. In a virtually identical complaint to the National Contact Point for the United Kingdom, multiple civil society organizations alleged similar violations against Gamma.[62] The National Contact Point accepted the complaint and released an initial assessment in June 2013, in which it was stated that: "while neither party has provided direct evidence about a supply by Gamma to Bahrain, the evidence provided suggests that the company's product may have been used against Bahraini activists. The [National Contact Point] considers that this substantiates the issues in respect of the company's obligations to do appropriate due diligence and to address impacts."[63]

[55] See Privacy International, "Criminal complaint to national cyber crime unit on behalf of Bahraini activists", 13 October 2014. Lawsuits against the NSO Group have also been filed in Israel and Cyprus: see David D. Kirkpatrick and Azam Ahmed, "Hacking a prince, an emir and a journalist to impress a client", *New York Times*, 31 August 2018.

[56] See European Centre for Constitutional and Human Rights, "FinFisher: no investigation into German-British software company", 12 December 2014.

[57] Amnesty International submission, p. 8.

[58] Ibid.

[59] Ibid.

[60] According to the organization's website, the main role of a National Contact Point "is to further the effectiveness of the Guidelines by undertaking promotional activities, handling enquiries, and contributing to the resolution of issues that may arise from the alleged non-observance of the guidelines in specific instances".

[61] See Privacy International, "OECD complaint: Trovicor exporting surveillance technology to Bahrain", 1 February 2013.

[62] See Privacy International, "German OECD NCP unwilling to investigate role of German company in human rights violations in Bahrain", 20 December 2013.

[63] United Kingdom, Department for Business Innovation and Skills, "Initial assessment by the UK National Contact Point for the OECD Guidelines for Multinational Enterprises: complaint from Privacy International and others against Gamma International UK Limited, June 2013" (London, 2013), para. 25.

45. Although the final report of the National Contact Point made several recommendations based on human rights standards, there is no evidence that Gamma has implemented them or even acknowledged the report.[64]

IV. Framework for the protection of fundamental rights against targeted surveillance

46. It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists. While human rights law provides definite restrictions on the use of surveillance tools, States conduct unlawful surveillance without fear of legal consequence. The human rights law framework is in place, but a framework to enforce limitations is not. It is imperative, urgently so, that States limit the uses of such technologies to lawful ones only, subjected to the strictest forms of oversight and authorization, and that States condition private sector participation in the surveillance tools market – from research and development to marketing, sale, transfer and maintenance – on human rights due diligence and a track record of compliance with human rights norms.

47. The previous mandate holder insisted that States should take measures to prevent the commercialization of surveillance technologies, paying particular attention to research, development, trade, export and use of these technologies, considering their ability to facilitate systematic human rights violations (A/HRC/23/40, para. 97). This call remains just as relevant today. In this section, the Special Rapporteur reviews the main elements of a framework to protect individuals from the uses of surveillance technology that interfere with the enjoyment of human rights. The steps proposed in the present report require action and implementation by: States, as users of these technologies and as exporting countries; by companies, in accordance with the Guiding Principles on Business and Human Rights; by States and companies working together with civil society; and by the Human Rights Council.

A. Moratorium on the export and use of targeted surveillance technologies

48. Private companies are creating, transferring and servicing – and States are purchasing and using – surveillance technologies in troubling ways. Credible allegations have shown that companies are selling their tools to Governments that use them to target journalists, activists, opposition figures and others who play critical roles in democratic society. Some of these companies object to the allegations, arguing that they do not permit the use of their products for illicit purposes, they have mechanisms to evaluate sales to "sensitive" end users and they abide by national laws on the control of exports. It is possible that companies are making genuine attempts to address the charges of complicity in surveillance-based repression and abuses. There is, however, no particular reason to take private companies at their word without subjecting them to public disclosure and accountability processes. The gravity of the allegations demands transparency in companies' relationships and processes, not to mention a range of other steps, which are described below.

49. Implementing the steps in the present report will take time. In the meantime, scores of journalists, activists, human rights defenders and government critics will be at the mercy of Governments emboldened by the array of highly intrusive surveillance tools at their disposal. It is therefore essential that companies immediately cease the sale and transfer of and support for such technologies, until they have provided convincing evidence that they have adopted sufficient measures (as outlined below) concerning due diligence, transparency and accountability to prevent or mitigate the use of these technologies to commit human rights abuses. Governments should also impose an immediate moratorium

[64] See Amitpal Singh, "OECD finds actions of Gamma International to be in violation of human rights", Citizen Lab, 3 March 2015; and "UK National Contact Point for the OECD Guidelines for Multinational Enterprises – Privacy International and Gamma International UK Ltd: final statement after examination of complaint", December 2014.

on granting licences for the export of surveillance technologies, until there is convincing evidence that the use of these technologies can be technically restricted to lawful purposes that are consistent with human rights standards, or that these technologies will only be exported to countries in which their use is subject to authorization – granted in accordance with due process and the standards of legality, necessity and legitimacy – by an independent and impartial judicial body. For now, however, the mounting evidence that privately developed surveillance tools are being used for manifestly illegitimate purposes offers a strong case for a moratorium on these transfers.

B. Obligations of Governments as users of surveillance technologies

1. Reinforce national laws limiting surveillance in accordance with the obligations of international human rights law

50. As a primary step, Governments deploying surveillance tools must ensure that they do so in accordance with a domestic legal framework that meets the standards required by international human rights law. Surveillance should only be authorized in law for the most serious criminal offences. To be compliant with those standards, national laws must:

(a) Emphasize that everyone enjoys the right not to be subjected to unlawful or arbitrary interference with his or her privacy and the right to hold opinions without interference and to seek, receive and impart information and ideas regardless of frontiers and through any media;

(b) Require that any legislation governing surveillance be contained in precise and publicly accessible laws and only be applied when necessary and proportionate to achieve one of the legitimate objectives enumerated in article 19 (3) of the International Covenant on Civil and Political Rights;

(c) Ensure that a surveillance operation be approved for use against a specific person only in accordance with international human rights law and when authorized by a competent, independent and impartial judicial body, with all appropriate limitations on time, manner, place and scope of the surveillance;

(d) Require, given the extreme risks of abuse associated with targeted surveillance technologies, that authorized uses be subjected to detailed record-keeping requirements. Surveillance requests should only be permitted in accordance with regular, documented legal processes and the issuance of warrants for such use. Surveillance subjects should be notified of the decision to authorize their surveillance as soon as such a notification would not seriously jeopardize the purpose of the surveillance.[65]

51. It is common for States to impose a high burden of proof on criminal investigations seeking access to the work of journalists (A/70/361, para. 24). Surveillance technologies are often used to target those who play significant roles in promoting democratic values. The Special Rapporteur recognizes that some States may believe that there are situations in which, for instance, journalists use the cover of their profession to engage in serious criminal offences. In his experience, these claims are almost always false or overstated. Too often, Governments use these sorts of claims to undermine journalism and dissenting voices or to target journalists for surveillance even when they are not the target of a legitimate criminal investigation, causing a disproportionate impact on the free press. In this context, the law's default position should be to prohibit the use of digital surveillance tools against individuals in the media. Of course, this does not provide journalists with immunity from other forms of legitimate legal process, including non-digital surveillance. It is simply that, in the context of the intrusive technologies of digital surveillance, the possibility of abuse or "leakage" from a legitimate criminal investigation into areas involving other journalistic work is very real and difficult, if not impossible, to contain. Its very possibility would likely serve to deter journalists from working on the most sensitive sorts of topics, not to mention the willingness of sources and whistle-blowers to come forward.

[65] See "Necessary and proportionate: International Principles on the Application of Human Rights to Communications Surveillance" (May 2014).

2. Establish public mechanisms for approval and oversight of surveillance technologies

52. Judicial authorization of government use of surveillance technologies is necessary but insufficient. The purchase of these technologies should also be subject to meaningful public oversight, consultation and control. In recent years, as the use of surveillance technologies has proliferated among law enforcement bodies in the United States, several communities have instituted civilian control boards to regulate their use and purchase. The city of Oakland in California, for instance, adopted an ordinance with several features regarding the purchase of surveillance technology that could be replicated by States.[66] These include:

(a) An approval process, carried out by the relevant departments, that takes into account the State's human rights obligations;

(b) Public notice of such purchases through regular processes, and public consultations on issues such as the human rights implications of such purchases and whether the technologies at issue will be effective at achieving their intended purposes;

(c) Regular public reporting on such approvals, purchases and uses.

53. Particularly in States that allow subnational organs a certain autonomy in the purchase of law enforcement tools, community control of such purchases should be encouraged and enforced. Given the clear public interest in maintaining the privacy and security of widely available commercial software, public oversight mechanisms should also be empowered to set policies on the stockpiling of vulnerabilities and the development of relevant exploits.

3. Provide victims with domestic legal tools of redress

54. For the reasons described above, it is difficult for the targets of unlawful or arbitrary surveillance to bring claims against Governments. Some of the barriers are structural, such as the unavailability in many legal systems for claims against government actors. Both legislatures and the courts may also bar these claims when they grant excessive deference to perceived national security and law enforcement interests. Some claims may be difficult to pursue because of the difficulty and expense of proving the existence of surveillance or attributing the surveillance to State actors – or even to specific State agencies that would be the targets of a lawsuit. Individual targets of surveillance often do not know of the surveillance being carried out against them – or, if they do, it may be beyond the tolling of a statute of limitations.[67] It is, in other words, extremely rare for a claimant to succeed in domestic legal claims arising from allegedly unlawful surveillance.

55. States that are serious about the abuse of surveillance technologies should take steps to enable individual claims against both State and non-State actors. This will, for many States, necessarily involve ensuring that the rules concerning jurisdiction, evidence, timeliness and other basic threshold conditions are fit for purpose in the digital age. They should, for instance, ensure that courts can accept and evaluate as evidence the forensic analysis of technical experts. National legislation should also establish causes of action against private entities that take into account changes in corporate ownership (known as "disposals" or "makeovers"), which often complicate the efforts of victims to seek accountability and redress.[68] Alternative forms of redress, such as truth commissions that enable victims of gross human rights abuses facilitated by digital surveillance to give testimony and that examine corporate complicity in these abuses, should also be considered.

56. At the same time, targeted surveillance is not always territorially contained. When States reach beyond their borders to conduct targeted surveillance, it may be difficult for the individuals targeted by such surveillance to bring claims against the offending State. Some of the same evidentiary and other burdens as in domestic claims may be present in

[66] See American Civil Liberties Union of Northern California, "Oakland becomes latest municipality to reclaim local control over surveillance technologies used by local law enforcement", 2 May 2018.

[67] See *Roman Zakharov v. Russia*.

[68] Access Now submission, p. 8.

these cases as well. Moreover, as in the *Doe* case noted above, courts may be unwilling to entertain lawsuits against foreign sovereigns. While the rules for such suits vary, States should interpret the norms of sovereign immunity to ensure that their courts may entertain suits against foreign Governments.

C. Obligations of Governments licensing export of surveillance technology

57. The Wassenaar Arrangement is not the final word on the control of exports of surveillance technologies; the enforcement of control lists depends upon national implementation. Neither does the Arrangement involve the participation of all major exporting countries: Israel, a major player in the surveillance technology market, claims that it is "fully compliant" with the Arrangement, although it has yet to become a participating State.[69] It is also a limited framework, since, notwithstanding its important objectives related to regional and international peace and security, it does not have a human rights orientation. Nonetheless, given that the Arrangement establishes standards that carry the expectation of broad implementation and compliance, participating States should leverage this valuable forum to impose rights-based limitations on the transfer of surveillance technologies.

58. In order to improve its role in developing global export standards, participating States would benefit from a human rights working group that could propose and consider standards for exports that integrate human rights concerns in technology transfers. But whether it adopts such a working group or other mechanism, it should develop a framework under which the licensing of any technology would be conditional upon a national human rights review and companies' compliance with the Guiding Principles on Business and Human Rights, as discussed below. As Privacy International put it, participating States, as well as other exporting Governments, should deny licensing "where there is a substantial risk that those exports could be used to violate human rights, where there is no legal framework in place in a destination governing the use of a surveillance item, or where the legal framework for its use falls short of international human rights law or standards".[70] To ensure compliance when export licences are denied on this basis, the surveillance technologies in question should be incorporated into existing sanctions regimes.[71]

59. While such standards would be valuable additions to the Wassenaar Arrangement, the ability of the public or specific civil society organizations to monitor their implementation will depend on stronger transparency obligations at the national and international levels. The Arrangement itself should promote such transparency by setting clear and enforceable guidelines for intergovernmental information-sharing and public disclosures concerning licensing standards, decisions to authorize, modify or reject licences, incidents or patterns of misuse of surveillance technologies and related human rights violations, and the treatment of digital vulnerabilities. National export laws should also allocate sufficient resources for public record-keeping and accessibility concerning export licensing decisions, and mandate relevant government agencies to solicit public input and conduct multi-stakeholder consultations when they are processing applications of export licences. Finally, States should also establish safe harbours for security research and exempt encryption items from export control restrictions.[72]

D. Companies' implementation of the Guiding Principles on Business and Human Rights

60. Given the extraordinary risk of abuse of surveillance technologies, the granting of export licences should be prohibited under domestic law unless a company regularly

[69] See Wassenaar Arrangement, "IL – Israel cybersecurity export control policy" (PowerPoint presentation), June 2016.

[70] Privacy International submission, p. 8.

[71] Ibid., pp. 3–4.

[72] Ibid., p. 5.

demonstrates that it has rigorously implemented its responsibilities under the Guiding Principles with respect to the design, sale, transfer or support of such technologies. This would effectively establish the Guiding Principles as preconditions for companies to participate in the surveillance market. In previous reports, the Special Rapporteur has explained how the information and communications technology sector should fulfil its responsibilities to respect human rights (A/HRC/35/22, paras. 45–75). For private surveillance companies to meet these responsibilities, they must develop, at a minimum, the following:[73]

(a) Customer policies that unequivocally affirm the responsibility of companies to respect freedom of expression, privacy and related human rights throughout their operations, and that client compliance with international human rights law is a condition for the approval and completion of a sale, transfer or contract of support;

(b) Human rights due diligence processes (such as human rights impact assessments) that are triggered when companies engage in activities that have a bearing on freedom of expression and privacy, such as the design, sale, transfer and servicing of surveillance products and services;

(c) Internal policies and standard contractual clauses that establish clear and specific prohibitions on product customization, targeting, servicing or assistance that violates international human rights law;

(d) Internal processes that ensure design and engineering choices incorporate human rights safeguards, such as flagging systems that detect misuse and kill switches that are triggered in the event of misuse;

(e) Regular programmes of audits and human rights verification processes to ensure that use of their products and services comply with international human rights law, including a commitment to publicly disclose key findings from these audits and verification processes;

(f) Notification processes that promptly report misuses of their tools to the relevant government oversight bodies (such as national human rights institutions) or intergovernmental bodies (such as special procedures complaints mechanisms);

(g) Transparency reporting that discloses the potential uses and capabilities of their products and the types of after-sales support provided, incidents of misuse and data concerning the number and type of sales to law enforcement, intelligence or other government agencies or their agents;

(h) Regular consultations with affected rights holders, civil society groups and digital rights organizations about the ongoing or potential impacts of their products and services and the human rights safeguards required to prevent or mitigate these impacts, with particular emphasis on engaging those at risk of surveillance-based discrimination or repression, such as racial and ethnic minorities and historically marginalized groups;

(i) Grievance mechanisms that enable individuals to submit complaints concerning human rights abuses facilitated by company products and services, and provide for independent assessment of those complaints and meaningful follow-up;

(j) Remedial mechanisms that enable complainants to seek compensation, apologies and other forms of redress, as appropriate, in cases in which complaints are independently verified.

E. Co-regulatory initiatives

61. The approaches of States and companies, as described here, may be insufficient to address the global problem of targeted surveillance. They also lack several important inputs – those of civil society actors, whether activists, technologists, academics, victims or those

[73] Many of these standards draw from the submissions of civil society, which can be found in the addendum to the present report and on the Special Rapporteur's website.

belonging to more than one of these categories. Co-regulatory governance that involves meaningful participation from State, business and civil society actors may provide a blueprint for human rights accountability in the private surveillance industry. In particular, co-regulatory initiatives developed to instil accountability and oversight among companies in the private security industry is instructive. Like private surveillance companies, the risks that private security companies assume are connected to their inherent involvement with State functions, particularly in the area of national security. Therefore, the co-regulation of private security companies requires efforts to educate companies about human rights concerns and creates incentives for multi-stakeholder participation (certification based on civil society-inclusive audit and monitoring processes), which may transfer well to the private surveillance industry.

62. Two aspects of the regulatory environment of private security companies are worth considering in the context of private surveillance companies. The Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict outlines recommendations for good State practices in such situations.[74] Although non-binding, it contains existing international law obligations for private security companies, as well as recommendations in the form of best practices for contracting States, territorial States and home States. Its principles of public disclosure and due diligence predate and mirror responsibilities found in the Guiding Principles.

63. The International Code of Conduct for Private Security Service Providers may also be an appropriate model. Established with the support of civil society, private industry and the Government of Switzerland, it is one of the few approaches that involves the participation of private security companies. The International Code of Conduct for Private Security Service Providers' Association is a multi-stakeholder initiative involving representatives from States, private security companies and civil society organizations. The non-binding Code is intended to supplement monitoring and oversight, articulating the international law obligations of companies and creating the structure of a framework for accountability to the Association. The Association consists of a general assembly, in which the stakeholder groups are represented, and a board of directors, which has 12 elected members who are representative of the three groups of stakeholders. Notably, company membership is contingent on compliance with the Code, including the Association's certification, auditing and verification processes.

64. As stated in the articles of association, the key idea of the Code is to promote the responsible use of private security services, as well as respect for international human rights law. The Code itself outlines both the general commitments of States and private security companies and other private security service providers, and specific principles for conduct in areas including: use of force, detention, apprehending persons, torture and other punishments, gender-based violence, human trafficking, slavery and forced labour, discrimination, and identification and registration of private security personnel.[75]

F. New focus in the United Nations on surveillance practices

65. The Human Rights Council has created, to real benefit, several working groups with mandates to address key themes on implementation of international human rights norms. The Council or its special procedures may consider a new mechanism to provide the kind of attention to specific cases that individual mandate holders may be unable to sustain and evaluate. A new working group, a cross-mandate task force, or a mandated plan of action could devote specific attention to claims that national surveillance practices – which touch

[74] See Switzerland, Federal Department of Foreign Affairs, and the International Committee of the Red Cross, "The Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict" (Berne, 2008).

[75] See also Sarah McKune submission, p. 10.

on many areas of human rights law and thus many mandates of special procedures – interfere with fundamental human rights.

V. Recommendations

66. **For States:**

(a) **States should impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place;**

(b) **States that purchase or use surveillance technologies ("purchasing States") should ensure that domestic laws permit their use only in accordance with the human rights standards of legality, necessity and legitimacy of objectives, and establish legal mechanisms of redress consistent with their obligation to provide victims of surveillance-related abuses with an effective remedy;**

(c) **Purchasing States should also establish mechanisms that ensure public or community approval, oversight and control of the purchase of surveillance technologies;**

(d) **States that export or permit the export of surveillance technologies ("exporting States") should ensure that the relevant government agencies solicit public input and conduct multi-stakeholder consultations when they are processing applications for export licences. All records pertaining to export licences should be stored and made available to the greatest extent possible. They should also establish safe harbours for security research and exempt encryption items from export control restrictions;**

(e) **Exporting States should join the Wassenaar Arrangement and abide by its rules and standards to the extent that these are consistent with international human rights law;**

(f) **States participating in the Wassenaar Arrangement should develop a framework by which the licensing of any technology would be conditional upon a national human rights review and companies' compliance with the Guiding Principles on Business and Human Rights. Such a framework could be developed through a specially established human rights working group. Additionally, they should set clear and enforceable guidelines on transparency and accountability with respect to licensing decisions, surveillance-related human rights abuses and the treatment of digital vulnerabilities.**

67. **For companies:**

(a) **Private surveillance companies should publicly affirm their responsibility to respect freedom of expression, privacy and related human rights, and integrate human rights due diligence processes from the earliest stages of product development and throughout their operations. These processes should establish human rights by design, regular consultations with civil society (particularly groups at risk of surveillance), and robust transparency reporting on business activities that have an impact on human rights;**

(b) **Companies should also put in place robust safeguards to ensure that any use of their products or services is compliant with human rights standards. These safeguards include contractual clauses that prohibit the customization, targeting, servicing or other use that violates international human rights law, technical design features to flag, prevent or mitigate misuse, and human rights audits and verification processes;**

(c) **When companies detect misuses of their products and services to commit human rights abuses, they should promptly report them to the relevant domestic, regional or international oversight bodies. They should also establish effective**

grievance and remedial mechanisms that enable victims of surveillance-related human rights abuses to submit complaints and seek redress.

68. **For the United Nations: the Organization, particularly the Human Rights Council, should create a working group or cross-mandate task force to monitor and provide recommendations on trends in, and individual cases of, human rights abuses facilitated by digital surveillance.**

69. **For all stakeholders: States, the private sector, civil society and other relevant stakeholders should establish co-regulatory initiatives that develop rights-based standards of conduct for the private surveillance industry and implement these standards through independent audits, and learning and policy initiatives.**