United Nations A/HRC/41/35/Add.3

General Assembly

Distr.: General
24 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

Overview of submissions received in preparation of 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 this addendum the Special Rapporteur provides a summary of issues and concerns raised by States, civil society and other stakeholders in their submissions to his report.

GE.19-08548(E)

1908548

Overview of submissions received in preparation of 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. Overview of submissions

1. This supplemental annex accompanies the June 2019 thematic report to the Human Rights Council of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression. With increasing frequency, governments are using privately developed technologies to hack into digital devices and spy on the online activities of civil society advocates, journalists, activists, academics, opposition figures and government critics. Such intrusive surveillance has reportedly facilitated the commission of human rights abuses offline, including arbitrary detention, torture and extrajudicial killings. The use of these technologies also interferes with the right to organize and assemble, both online and offline. In his report, the Special Rapporteur evaluates the human rights obligations of States and the responsibilities of companies concerning the sale, licensing and export of private surveillance technologies.

2. A call for submissions was issued on 18 December 2018, and requested input from States and civil society to share information concerning the regulatory frameworks that may be applicable to the development, marketing, export, deployment, and/or use of surveillance technologies by private companies.[1] Eleven States and thirty-three non-governmental groups and individuals made submissions to the Special Rapporteur. The Special Rapporteur is grateful for all the submissions he received.

3. This annex provides a summary of issues and concerns raised by States, civil society and other stakeholders in these submissions. Readers are encouraged to look at the submissions themselves for more detailed information. This annex should also be read in conjunction with the Special Rapporteur's report, which articulates principles that he believes should guide the regulation of the private surveillance industry. Finally, this annex reflects only the submissions received and should not be understood as a broader literature review related to the topics discussed in the main report.

II. Private surveillance tools

4. A majority of the submissions focus on malware, spyware, and other types of dual-use technologies that are manufactured, sold, and serviced by private surveillance companies and used by governments to target members of civil society. Many of these tools have been discussed in the main report. This section elaborates on some of these discussions, and describes additional trends and concerns raised in the submissions.

Intrusion Software

5. Private surveillance companies use intrusion software to break into a target system and to monitor activity on the device and access as well as download information off the device. Companies usually send socially engineered messages to trick a target into clicking on a malicious link, but some forms of intrusion software, known as "zero-click technology," can be installed on a device without any action from the target (NYU Global Justice Clinic ("GJC"), 7). The producers of intrusion software most frequently mentioned in the submissions we received are NSO Group, Hacking Team, FinFisher, Cyberbit, and M.L.M. Protection.

6. NSO Group is an Israeli Q Cyber Technologies company, with headquarters in Luxembourg, and currently owned by Novalpina Capital (Citizen Lab, 6-8). Citizen Lab found that the company may have sold intrusion spyware to government agencies in 45 countries, and there is evidence that at least six of those countries have used spyware to monitor civil society. (Citizen Lab, 8) The most well-known product sold by NSO Group appears to be Pegasus, a type of spyware. *Id.* The Saudi regime may have used Pegasus to track the communications of the journalist Jamal Khashoggi before his murder. (*Id*; Human Rights Foundation ("HRF"), 4).

[1] https://freedex.org/2018/12/13/call-for-submissions-the-surveillance-industry-and-human-rights/.

7. FinFisher sells tools similar to NSO Group's Pegasus. FinFisher is a private surveillance company based in Munich, Germany, and was previously part of the UK-based Gamma Group. FinFisher's command and control servers (computers that attackers use to send commands to target systems compromised by malware) have been identified in 25 countries, including the United States. (Citizen Lab, 10-11) One of the most well-known FinFisher products is FinSpy, a tool that has been used by governments to intercept and monitor the activities of human rights activists, journalists, and opposition leaders. (*Id.*, 9 - 10)

8. Hacking Team is an Italian private surveillance company backed by "private investment" which manufactures "offensive technology" technology and "lawful interception " tools to law enforcement agencies around the world and has been identified in at least 21 countries. (Citizen Lab, 10; Sarah McKune, 5). Hacking Team is also linked to a new company called Grey Heron, which markets itself as a technology company that provides "lawful access" to the most popular encrypted services (Access Now, 9). One of the most well-known Hacking Team products is the company's Remote Control System (RCS). RCS can intercept and transmit data from a target's infected phone or computer before the data is transmitted or encrypted. Additionally, RCS can turn on a device's webcam and microphone as well as record emails, instant messages, information typed into a Web browser, and record video calls (Citizen Lab, 10). The Ethiopian government has reportedly used RCS to target Ethiopian American journalists and activists. (*Id.*). Cyberbit has also been found to target researchers and Ethiopian academics and activists.

9. Cyberbit is an Israeli cybersecurity company owned by Elbit Systems. It sells the PC Surveillance System (recently renamed PC 360), which can "monitor and extract information including VoIP, calls, files, emails, audio recordings, key logs and virtually any information available on the target device." (Citizen Lab, 9) Its products has been linked to spyware attacks on dozens of activists, researchers and journalists. (*Id.*; Committee to Protect Journalists (CPJ), 3)

10. M.L.M. Protection Ltd. is an Israeli surveillance firm that sells "long-range interception technology" which allows customers to record a wide range of content, including text messages and communications sent through popular messaging services such as WhatsApp. (Derechos Digitales, 2). The former President of Panama, Ricardo Martinelli reportedly purchased approximately 13.5 million dollars in private surveillance technologies from M.L.M. Protection Ltd. and NSO Group between 2009 and 2014, and is currently facing criminal charges for spying on approximately 150 individuals "including journalists, businessmen, civil society leaders and members of the opposition." (AI Sur, 9).

Social Engineering

11. The main report discusses how the effectiveness of malware attacks is enhanced through the use of social engineering techniques. The malware attack on Omar Abduaziz Alzahrani, a Saudi human rights activist living in Canada, is a paradigmatic example of how social engineering techniques have advanced. On the day that he made an online Amazon purchase, Mr. Alzahrani received a text message with the domain link Sunday-deals[dot]com disguised as a shipment notification. On closer examination, however, Citizen Lab identified the exploit domain as part of Pegasus's spyware suite (HRF, 4). Human rights defenders, journalists, and political activists in Azerbaijan have also been targeted through e-mails impersonating their colleagues (Amnesty International, 17). Rasul Jafarov, a prominent lawyer and human rights defender, was told by friends and colleagues that they received an email about political prisoners from an e-mail address similar to Jafarov's and that included an attachment infected with malware. If clicked, the attachment would have installed a keylogger recording the user's keystrokes and malware that would send screenshots of targets' computers back to the attacker. The target would not necessarily be aware of the infection because after the attachment was clicked, "the malware also opened an Office document in Azeri dealing with political prisoners." (Amnesty International, 16).

12. Elaborate social engineering campaigns have also been designed to lure targets to click on malicious links on websites and social media. (Access Now, 6). In Turkey, during the March for Justice in July 2017, FinFisher attackers impersonated the social media

accounts of protesters to promote a link to a malware infected website disguised as the official website belonging to March for Justice. (*Id.,* 4). The attackers promoted the site using popular hashtags and retweets of legitimate content, and also shared the link on the March for Justice Facebook group. (*Id.*, 3-6).

Deep Packet Inspection

13. Deep Packet Inspection (DPI) tools are tools that allow users to monitor and analyze all traffic passing through internet and telecommunications networks. Governments are able to block access to websites by either redirecting network users to download infected versions of popular software, including antivirus software, or adding malicious traffic to Internet connections to prevent networks users from accessing a website the government wants to block. Narus and Sandvine, which are based in the U.S., have sold DPI tools to the government of Egypt. Civil society fears that these tools are being used in the government's ongoing crackdown on journalists. (CPJ, 3 - 4) Sandvine's DPI products have also been linked to the censorship of websites belonging to the media or opposition parties in Egypt and Turkey. (Association for Freedom of thought and Expression, Egypt ("AFTE"), 6)

Large-Scale Monitoring Software

14. In addition to developing tools that target specific devices or accounts, some companies help governments build and operate systems capable of large-scale surveillance. Verint Systems and NICE Systems, based in Israel, develop and sell monitoring center platforms that enable governments to monitor and intercept internet traffic across all domestic networks. This "critical interception infrastructure" has reportedly been sold to the government of Colombia. (CPJ, 4-5; Al Sur, 3). Nexa, previously named Amesys and based in France, sells both large-scale monitoring centers and targeted surveillance tools (International Federation for Human Rights ("FIDH"), 2-3; AFTE, 6). Amesys' large-scale monitoring software Cerebro allows authorities to engage in "a comprehensive surveillance of communications through DPI, including voice calls, text messages, e-mails, instant messages, social networks, and search engine searches." (AFTE Submission, 5). This software has been linked to attacks on civil society and other human rights abuses in Libya and Egypt. (Privacy International, 5; FIDH, 2). In Brazil, Digitro Tecnologia designs and sells monitoring systems that "allo[w] up to 30 people to work simultaneously on mobile phones, landlines and emails." The government of Uruguay and the Brazilian Federal Police are reportedly customers. (Derechos Digitales, 2).

International Mobile Subscriber Identity-catchers

15. International Mobile Subscriber Identity-catchers (IMSIs) intercept mobile communications by mimicking the strongest nearby cell tower where they are located and draw the connection of personal communication devices. The connection allows IMSI-catchers to acquire data that observers may use to monitor telephone calls and location data. IMSI-catchers have widespread use, often by law enforcement and intelligence agencies (International Network of Civil Liberties Organizations, 8). The use of IMSIs has been documented in United States, Canada, Ireland, the United Kingdom and South Africa (*Id.*, 8-9). In South Africa, IMSI-catchers are deployed without judicial oversight (ALT Advisory and Right2Know Campaign, 12). IMSI-catchers and other tools were also used in the Philippines to "hunt down and kill dealers and addicts" as part of the government's war on drugs (Southeast Asian Press Alliance ("SEAPA"), 1).

Biometric Surveillance

16. In China, companies develop, export, and facilitate an extensive range of surveillance technologies including biometrics identification systems, and facial recognition and gait recognition software (Human Rights in China ("HRIC"), 1). Gait recognition developed by the Chinese company Watrix, for example, identifies individuals by the manner in which they walk (Chinese Human Rights Defenders ("CHRD"), 2). In Paraguay, facial recognition systems are being used to monitor downtown areas and football stadiums. (AI Sur, 5- 6). In Brazil, facial recognition software has been deployed to "prevent fraud on buses" and in airports and public schools. (Internet Lab, 6 - 7). In 2014, Venezuela

implemented a biometric system that requires the fingerprint enrollment of individuals seeking to buy food and medicine at regulated prices. Initially optional, this system eventually became mandatory for citizens. (AI Sur, 7).

Drone Surveillance

17. In Brazil, drones have been used to collect information about people, cars, and buildings, with the capability of tracking demonstrations and activists. (AI Sur, 7) Surveillance drones and balloons have also been deployed in Chile to monitor crowded places and events in the name of safety; however, they have also been "used to constantly surveil and repress indigenous communities in the south of the country in recent years." (*Id.*, 7 - 8) The government of India has also deployed surveillance drones in Kashmir. (Association of Parents of Disappeared Persons ("APDP"), Jammu Kashmir Coalition of Civil Society, and Srinagar, Indian-Administered Jammu and Kashmir, 3) In China, companies develop and sell drones as part of a broader suite of surveillance products. (HRIC, 1).

Role of Information Technology Companies

18. IT companies that do not specialize in surveillance may nevertheless be engaged in the development and sale of technology products that support the development and enhancement of surveillance systems. In India, law enforcement acquired software from Wipro, a major Indian IT company, to create a digital database of "First Information Reports (FIRs), case dairies [sic], crime details forms, arrest memos, and police station dairies [sic]" as part of the country's Crime and Criminal Tracking Network System (CCTNS). (APDP et al., 2; see also Center for Communications Governance ("CCG"), 10) Civil society fears that the CCTNS is being used to "profile individuals using their past conduct, which now can include all stages of an investigation and not just a conviction by a court of law to profile individuals on the basis of past crimes" and that it will "be leveraged into carrying out more invasive surveillance of the public at large." (APDP et al., 2) It is "doubtful whether the company has any control over the manner in which the CCTNS is utilized by law enforcement agencies." (CCG, 17)

Arms Manufacturers

19. In addition to being the UK's largest arms manufacturer, BAE Systems exports controlled surveillance tools. BAE's mass surveillance software has been exported "to countries where human rights abuses are common, including to Saudi Arabia, UAE, Qatar, Oman, Morocco, and Algeria." (Privacy International, 7). There is also evidence indicating that BAE surveillance software was sold to the government of South Africa (ALT Advisory et al., 6).

Mass Surveillance

20. While the Special Rapporteur's report does not address the problem of mass surveillance, several submissions note that governments frequently conduct this form of surveillance under vaguely formulated domestic frameworks that do not adequately protect human rights and even outside existing law. (See e.g. AFTE, 1-3; Institute for Human Rights and Business ("IHRB"), 7)

III. Relationship between the government and the private surveillance industry

21. Submissions raise concern about the close relationship between States and the private surveillance industry and argue that the influence of the private sector hinders "both an improvement of regulations as well as stricter decision about export licenses." (Reporters Without Borders ("RSF"), 5.) For example, NSO Group's Pegasus spyware was developed by the alumni of Unit 8200, Israel Defense Force's elite intelligence unit. (McKune, 7.) The private sector also reportedly partners with governments to host annual trade shows to exhibit surveillance-related products (AI Sur, 3). Some governments even

use public funds to support the design of surveillance technologies. For example, the government of South Africa has reportedly provided funding to VASTech SA (Pty) Limited, a private surveillance company that designs and sells mass surveillance hardware and software. In 2011, reports surfaced that the company had sold surveillance products to the Gaddafi regime in Libya. (ALT Advisory et al., 9).

IV. The obligations of states

The Wassenaar Arrangement

22. Currently, there are very few systems that govern cross-border transfers of surveillance technology. As the main report illustrates, the Wassenaar Arrangement provides guidelines and norms for export of the items on the List of Dual-Use Goods and Technologies and the Munitions List. (Access Now, 1) The Wassenaar Arrangement, a voluntary body with 42 participating states, aims to "contribute to regional and international security and stability, by promoting transparency and great responsibility" and "keep these powerful tools from those who would counter the coalition's goals." (Access Now, 1)

23. Under the Wassenaar Arrangement, the members agree to apply export controls to the List, which includes dual-use technology such as surveillance tools. (Access Now, 1). For example, in 2010, "laser microphones," which are used to eavesdrop on conversation, were added to the list and in 2012, phone monitoring technology was added to the list to control mobile and satellite phone monitoring equipment. (Privacy International, 4) The List further expanded in 2013 with inclusion of intrusion software and internet monitoring technology, and the additions were aimed at "surveillance and law enforcement/intelligence gathering tools and Internet Protocol (IP) network surveillance systems or equipment, which, under certain conditions, may be detrimental to international and regional security and stability." (Privacy International, 5).

24. Some members, like EU States, have incorporated substantial parts of the Wassenaar Arrangement while other States such as Argentina and have not proactively implemented the provisions of the agreement. (AI Sur, 4) Furthermore, there are non-participating members of the Wassenaar Arrangement, such as Israel, that have included items from the Wassenaar Arrangement's control list to its own list of controlled goods. (Privacy International, 6.)The following section discusses the export regimes of some of the members of the Wassenaar Arrangement.

EU Framework

25. Several submissions discuss the EU's export control regime established under Regulation (EC) No 428/2009 and the recent efforts to review and update the framework. EU export controls were initially established to regulate weapons of mass destruction but was expanded to include dual-use technology including cyber-surveillance technologies. (Access Now, 1) Recognizing the increasing risks of cybertools for mass surveillance, monitoring, tracking and interception and their impact on human rights, the European Commission proposed a review of the current export control regime. (Access Now, 2; Privacy International, 6) Some of the recent developments include establishment of a Subcommittee, the Surveillance Technology Working Group (STEG), which is tasked with identifying surveillance technology that poses risk to human rights and the effective ways to control them. (Privacy International, 6) The 2013 additions (intrusion software and internet monitoring technology) to the Wassenaar list were also added into the EU Dual Use regulation in January 2015. (*Id.*, 5)

26. However, submissions expresses concern that because any changes to the regulation requires unanimous approval by the EU members, progress is slow and the text of the reform is yet to be finalized. (Amnesty International, 5; Privacy International, 6.)

Domestic Export Control Laws

27. Several submissions discuss domestic laws implemented by both the members and non-members of the Wassenaar Arrangement. Many submissions reflect efforts by some

States to strengthen their existing frameworks. For example, while the United States has not fully incorporated the 2013 amendment to the Wassenaar Arrangement, the U.S. Commerce Department may "propose new export controls designed to protect human rights." Furthermore, the "Commerce Department is simultaneously undertaking a broad review of export controls for new technologies" in light of "emerging technologies." (Electronic Privacy Information Center, 2) In addition to implementing its obligations under the EU export control regime, the government of Germany states that it has also established "national legislation in order to control certain cyber-surveillance items," including mandatory export license requirements for "companies which export certain products that are used for cyber-surveillance purposes in mobile radio and terrestrial networks." (Germany, 1). It has also restricted the "supply of certain technical assistance by a German citizen in third countries," which now requires an authorization. (*Id.*) The government of the United Kingdom has expressed its commitment to a strong export control regime, stating that it takes into consideration "[c]oncerns about internal repression, regional instability or other human rights violations, "concerns about the development of weapons of mass destruction," "foreign policy and international treaty commitments including those resulting from the imposition of EU or United Nations trade sanctions or arms embargoes," and the need to ensure the national and collective security of the UK and its allies." (United Kingdom, 1)

28. Despite these examples, many submissions indicate that efforts to strengthen export controls are the exception rather than the rule and, in any case, have done little to alter the weak and fragmented state of export controls. In Latin America, for example, there is still an "overall lack of clear, precise, unambiguous and detailed laws, administrative regulations, judicial decisions and/or other policies to regulate the export, import and use of surveillance technology." (AI Sur, 2) Membership in the Wassenaar Arrangement has had "little meaningful effect" on the surveillance practices of Argentina and Mexico. (*Id.*)

Sanctions

29. In addition to the legal frameworks discussed above, sanctions have been used to control transfer of some surveillance technologies. For example, Council Regulation (EU) 36/2012 imposed a ban on the sale, supply, transfer or export of "surveillance equipment, technology or software whether or not originating in the Union, to any person, entity or body in Syria or for use in Syria." (Privacy International, 3) Similar sanctions have been imposed on the sale of surveillance technologies to Iran. (*Id.*)

V. Criticisms of existing frameworks

Vague International Standards

30. Several submissions indicate that existing frameworks contain overbroad language that precludes effective regulation of the transfer of surveillance tools and creates potential loopholes for surveillance companies to exploit and circumvent licensing requirements. (RSF, 4; Amnesty International, 5) The issue may be that Wassenaar and the EU Framework were historically created for completely different items such as nuclear goods or components of weapons of mass destruction, and therefore it is difficult to come up with a balanced legal language that "fits for both surveillance technology and "traditional dual use items" (RSF, 4)

31. The lack of clear international standards leads States to adopt contradictory licensing decisions. Even within the EU, States may reach different decisions about certain technologies and which countries they may be exported to. (RSF, 5) The problem of inconsistent standards is further aggravated by the fact that the authorities often depend on non-public information gathered by the national intelligence agencies and for this reason, refuse to participate in intergovernmental intelligence sharing. (*Id.)*

Inadequate Consideration of Human Rights

32. This lack of clarity also guides States away from human rights considerations, and towards highly subjective "geopolitical and strategic deliberations." (RSF, 5) The close

business relationships between States and private surveillance companies also hinders the development and implementation of principled, rights-oriented regulation. (*Id.*) For example, the risk assessments that several EU States conduct have not stemmed the tide of surveillance exports to States where such tools have been used to violate human rights. (Amnesty International, 6; Privacy International, 7) Even the proposed reforms to the EU framework contain "unduly narrow definition of human rights and fails to require that states deny license for surveillance exports that pose human rights risks." (Amnesty International, 5)

Lack of Transparency

33. In addition to inadequate international and national export control measures, several submissions identify the lack of transparency as a major problem. States, whether members of Wassenaar or not, generally do not exchange information on their licensing standards and decisions with other States. (Sarah McKune, 5) Even where States disclose information about licensing decisions and export control measures, "this practice is far from uniform, and within the EU efforts to establish more substantive reporting through export regulations have stalled." (*Id.*) 11 EU members, including France and Italy, refuse to make any licensing data available to public. (Privacy International, 6) This lack of transparency may be attributable to "the broader ecosystem of private financing that fuels much of the industry." (Sarah McKune, 8) Since companies are funded by private investors, key strategic decisions, including company's approaches to human rights, are formulated behind closed doors. The limited public information available about the private surveillance industry has mainly surfaced as a result on civil society and academic research and investigative reporting. (*Id.*, 5) But even these sources are under threat, as NGOs, academics, journalists and public interest lawyers are harassed, censored, surveilled, attacked and blacklisted. (*Id.*; see also Center for Legal and Social Studies ("CELS"), 4)

34. Submissions argue that the lack of transparency has various implications for human rights. Even in countries that "provide an element of transparency into licensing procedures, the limited information made public makes it difficult to scrutinize the adequacy of these procedures." (Amnesty International, 6.) Despite the cutting-edge forensic research provided by NGOs, academics, journalists and others, such material is still unable to provide a comprehensive picture of how targets are hacked or spied on, and how their surveillance is linked to other human rights abuses. This makes it difficult for victims to obtain evidence necessary to bring litigation and precludes meaningful public scrutiny and oversight. *Id.*

Overbroad Domestic Surveillance Laws

35. Domestic surveillance laws are frequently overbroad and vague, giving the authorities wide discretion to deploy high-tech surveillance tools. China's "far-reaching and draconian Cybersecurity Law," for example, provides authorities with "broad powers to restrict and penalize online expression" and also ban VPNs "without government pre-approval." (CHRD, 1.) Human rights defenders fear that this law provides the government with broad authority to deploy a host of invasive surveillance tools including data extracting technology, facial recognition software, and "grid management" police surveillance systems. (*Id.*) Cybersecurity and computer crime laws that provide government authorities with broad powers to conduct surveillance have also been enacted in the Philippines, Singapore, Thailand and Vietnam. (SEAPA, 1-6.) Even if these laws were "sufficiently clear," they may still fail to meet the standards of necessity, proportionality and legitimacy of objectives. (GJC, 9)

36. While several States ban unauthorized surveillance, these restrictions generally do not apply to government surveillance. Azerbaijan's Criminal Code, for example, imposes "criminal liability for using technical means provided for obtaining information secretly by persons who are not authorized." (Azerbaijan, 2.) In Russia, Article 24 of the Constitution states that the "collection, holding, and use and spread of information about one's private life, without his authorization, are not permissible." (Russia, 1) However, neither of these restrictions address the problem of legally authorized surveillance that is overbroad and repressive. Constitutional protections of the right to privacy also frequently beg the

question. In Brazil, "although the secrecy of communications is protected under the Brazilian Federal Constitution, there is significant dispute around the standards of protection conferred to different types of communications data." (Internet Lab, 2.)

VI. Recommendations to states

Explicit Focus on Human Rights

37. Export control frameworks should include an explicit focus on human rights. In particular, States should be required to deny licenses for exports that carry a "substantial risk" that they will be used to harm human rights. (PI, 8) Such standards should be shored up with effective and independent monitoring and oversight mechanisms, sanctions against companies that fail to comply, and human rights due diligence requirements for companies. (GJC, 13; RSF, 5; Privacy International, 8; Amnesty international, 7) The minimum human rights standards companies should meet are detailed below.

Increase Transparency

38. To address these issues and develop definitions and standards that are fit for purpose, States should provide more information about their current licensing practices. States should, for example, install "a mechanism of intergovernmental information sharing about the human rights situation in destination countries, previous decisions for certain technologies and countries and about the previous use of surveillance technology in the country." (RSF, 5)

Ongoing and Dynamic Review of Regulatory Standards

39. States should engage in periodic review of relevant frameworks to ensure they cover all relevant surveillance technologies. (IHRB, 19; Privacy International, 8) Furthermore, states must note that as the technology continues to evolve and the challenges become far more complex, updates to the frameworks should take into consideration the expertise of all stakeholders including civil society, researchers, and international human rights advocates. (Privacy International, 8; Citizen Lab, 19)

Protecting Security Research

40. In regulating transfers of invasive surveillance tools, States should establish clear definitions of surveillance technology that contain "clear and enforceable" safeguards to protect legitimate security research and communication technologies. (Privacy International, 8)

VII. The Human Rights responsibilities of companies

41. Submissions also raise concerns about the lack of corporate human rights accountability. Private surveillance companies routinely deny, or simply ignore, questions about alleged human rights violations, citing concerns about their government clients' privacy and confidentiality. (Sarah McKune, 4-5) Many companies also do not "have in place policies and practices that are purposefully inline with the Guiding Principles on Business and Human Rights." (Center for Internet & Society, India ("CIS"), 10) Those that have made minimal commitments to human rights continue to supply surveillance products and services to governments that have a track record of using them to commit human rights abuses. (Sarah McKune, 9)

42. Submissions highlighted a variety of recommendations that would bring companies in line with the UN Guiding Principles; most of these recommendations are reflected in the main report. A few additional points are worth highlighting here. With respect to human rights due diligence, companies should conduct human rights impact assessments and make commitments to refuse entering into business with "countries that have a history of targeting human rights defenders." (GJC, 14) Additionally, "[r]obust multistakeholder initiatives, rooted in the UN Guiding Principles and in which industry plays a key role,

could be instrumental in encouraging a "race to the top" to fulfill the corporate responsibility to respect human rights." (Sarah McKune, 9) As the main report illustrates, the private military and security company (PMSC) industry offers a model for multi-stakeholder governance. (*Id*.) Ultimately, however, it is questionable whether the UN Guiding Principles provide a sufficient framework. It was suggested that "if industry participants consider that they cannot address human rights impacts without ultimately rendering their business unprofitable, perhaps that is a sign that digital espionage functions should remain inherent to the state and out of the hands of the private sector." (*Id.*)

VIII. Remedies

43. The submissions go into detail about the lack of effective remedial mechanisms available to individuals harmed by the use of surveillance technologies. States consistently fail to investigate complaints of wrongdoing by private surveillance companies. (Amnesty International, 7) In the rare instance that inter-governmental bodies investigate complaints, they lack the ability to compel companies to cooperate or enforce their recommendations. For example, a joint civil society complaint before the U.K. National Contact Point of the Organization for Economic Cooperation and Development (OECD) triggered an investigation into the practices of Gamma Group, the firm that produced Finfisher. Although the U.K. National Contact Point found that "Gamma's conduct was inconsistent with its responsibilities under the OECD Guidelines, it was unable to confirm that Gamma caused or contributed to the human rights abuses alleged." Its investigation was limited in part because Gamma refused to cooperate. (*Id.*, 7)

44. It is frequently difficult to identify an appropriate legal remedy for surveillance-related harms, and even where there is a remedy, there is no meaningful means of enforcement. (*Id.*) In the context of litigation, "[u]ncertain jurisdiction, corporate liability shields, sovereign immunity, lack of technical evidence, restrictive contracts, and official impunity" routinely deny victims effective legal remedies. It may also be difficult to articulate or quantify the harms individuals suffer as a result of digital surveillance, since these often transpire as "fear, uncertainty and actions not taken." (GJC, 12) Nevertheless, documented chilling effects and financial costs associated with technical circumvention measures may create bases for remedy. (*Id.*)

45. Government secrecy frequently stands in the way of an effective remedy. Restrictions on the public disclosure of information regarding government surveillance activities, such as those prohibiting service providers to disclose "information about government requests and orders" under India's Information Technology Act Rules, hinder investigations into surveillance-related abuses. (CIS, 4; see also CELS, 4) Domestic laws that authorize government surveillance on wide ranging national security grounds also effectively immunize them from legal accountability. (Bytes for All, 2 - 3)

46. A few submissions explored the possibility of remedies other than litigation. Guarantees of non-recurrence may be a critical and appropriate remedy in the context of digital surveillance. (GJC, 12) States should also ensure that "authorities charged with overseeing the export of surveillance technologies have sufficient authority, independence and transparency to ensure adequate scrutiny of human rights risks." (Amnesty International, 9) International bodies, including human rights mechanisms, should undertake further research and analysis into how the right to effective remedies can be vindicated in this context. (GJC, 12)