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

REFERENCE:
OL USA 23/2019

8 November 2019

Mr. Cassayre,

I have the honour to address you in my capacity as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pursuant to Human Rights Council resolution 34/18.

I am writing to provide my preliminary reactions to the draft U.S. Government Guidance for the Export of Hardware, Software and Technology with Surveillance Capabilities and/or parts/know-how ("draft Guidance"). I welcome the State Department's recognition of the problems arising from the widespread use of surveillance technologies for purposes that are inconsistent with international human rights law. I especially welcome this effort to highlight steps companies should take to mitigate the threats to human rights raised by private surveillance technologies. I am gratified that the Department has sought input from various stakeholders through an open comment process, and I am happy to provide preliminary reactions to this effort to encourage the private sector's incorporation of human rights principles.

The initiative by the State Department to engage closely with human rights mechanisms to govern tools with surveillance capabilities comes at a critical juncture. Credible reporting by media and human rights organizations has illuminated how surveillance technologies are frequently used by governments to track and silence civil society journalists, political dissents, and others. Special procedures mandate holders have also reported the use of such technologies contrary to human rights law and illustrated the troubling effects of such use on human rights including, but not limited to, the rights to freedom of expression and privacy. My most recent report to the Human Rights Council raised concern for the current lack of framework for oversight in the surveillance industry and urged States and private companies to take meaningful steps to increase accountability.[1]

For this reason, the draft Guidance, which seeks to "assist exporters of items with intended and unintended surveillance capabilities [in the] implementation of the UN Guiding Principles on Business and Human Rights as well as the OECD Guidelines for Multinational Enterprises," is particularly valuable. It recognizes the responsibility of businesses, under the UN Guiding Principles, to respect human rights, independent of State obligations. The draft Guidance encourages companies to adopt public statements

[1] *See generally* David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, U.N. Doc. A/HRC/41/35 (May 28, 2019), https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/41/35.

of commitment to respect human rights; implement rigorous due diligence processes; mitigate risks of misuse through contractual and procedural safeguards; and provide for remediation of human rights violations.

In addition, I would like to commend the Department for highlighting the human rights responsibilities of exporters of items with *intended* surveillance capabilities and exporters of items with *unintended* surveillance technologies. The draft Guidance covers items already listed on the Commerce Control List the International Traffic in Arms Regulations, as well as technologies with incidental or peripheral surveillance capabilities such as social media analytics software, rapid DNA testing, crypto-analysis products, penetration-testing tools, information technology products with deep packet inspection functions, and recording devices that can be accessed remotely. The inclusion of tools with unintended surveillance capabilities in the draft Guidance was a meaningful reminder of the highly sophisticated and flexible nature of digital products and of the responsibility of technology companies to conduct robust due diligence to safeguard against both intended and unintended use of their products in violation of human rights law.

I would like to share the following specific comments:

I. Human Rights Standard

The draft Guidance seeks to "assist exporters of items with intended and unintended surveillance capabilities with implementation of the UN Guiding Principles on Business and Human Rights (UNGPs) as well as the OECD Guidelines for Multinational Enterprises (Guidelines)" and recommends exporters to implement due diligence policies "based on the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the OECD Guidelines for Multinational Enterprises, and the UN Guiding Principles on Business and Human Rights."

I welcome the Department's promotion of a rights-based approach to the regulation of the surveillance industry and would only add a few points of emphasis. Given the extraordinary risk of the misuse of surveillance products, it is my view that the commitment to human rights must be clearly articulated in company policies, and full incorporation of the Guiding Principles should be a precondition for companies to participate in the surveillance market. The policies and standards adopted by the companies should be sufficiently tailored and comprehensive, given the scale and complexity of the industry and the severity of adverse human rights impacts.

Furthermore, the rights-based policies must be instrumental in the company's decision-making processes. For example, the companies must be strongly recommended to give decisive weight to their due diligence assessments and to establish the policy of refusing sales or service of their products when there is a substantial risk of misuse, when there is no legal framework in place, or when the legal framework of the government end-user falls short of international human rights law or standards.

Finally, I recognize that it takes time to implement the steps articulated in the draft Guidance, such as building human rights policies, designing and implementing due diligence mechanism, understanding the full capabilities of the export in question, and creating effective and safe channels of communication and grievance mechanism. And yet, in this interim period, journalists, activists, human rights defenders and political dissidents are exposed to the serious threats posed by highly intrusive surveillance tools. Therefore, in my 2019 report, I urged companies to immediately cease the sale and transfer of and support for such technologies, until they provide convincing evidence that they have adopted sufficient measures to align their practices with international human rights standards.[2] It follows that States must also impose an immediate moratorium on granting licenses for export of surveillance technologies until proper protections and oversight systems are established and implemented.

II. Due Diligence in Line with International Human Rights Standards

The draft Guidance recommends that exporters of surveillance technology "review whether the government end-user's laws, regulations, and practices that implicate items with surveillance capabilities are consistent with the ICCPR," in conjunction with the end-user's human rights record. For instance, according to the draft, companies should "[r]eview laws, regulations, or practices that may unduly hinder freedom of expression, and/or interfere unlawfully or arbitrarily with privacy, as feasible"; "[r]eview laws, regulations, or practices concerning government interception of private communications, and government access to stored private communications, as feasible"; "[r]eview the extent to which the Government implements its laws on surveillance and the oversight mechanisms in place, as feasible"; and "[r]eview the IT infrastructure of the export destination country to determine level of government access and/or control, as feasible."

As illustrated by the draft Guidance, companies conducting due diligence of a government end-user should consider whether the legislation and regulations governing surveillance are consistent with the International Covenant on Civil and Political Rights ("ICCPR"). Such laws must be precise and publicly accessible, and only be applied when necessary and proportionate to achieve one of the legitimate objectives enumerated in article 19 (3) of the ICCPR.[3] The requirement of necessity implies an assessment of the proportionality of restrictions, with the aim of ensuring that restrictions "target a specific objective and do not unduly intrude upon the rights of targeted persons."[4]

---

[2] Id. at ¶¶ 48-49.

[3] U.N. Human Rights Committee, General Comment No. 34, art.19, ¶ 25, U.N. Doc. CCPR/C/GC/34, (Sept. 12, 2011), http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

[4] David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, ¶ 35, U.N. Doc. A/HRC/29/32 (May. 22, 2015), https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement; *see also* U.N. Human Rights Committee, General Comment No. 27, art. 12, U.N. Doc. CCPR/C/21/Rev.1/Add.9 (Nov. 1, 1999), http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f21%2fRev.1%2fAdd.9&Lang=en

In keeping with these standards, the exporters of technologies with surveillance capabilities should conduct a genuine and thorough examination of the Government end-user's legal framework before the sale and throughout the life cycle of the product. For example, it is not enough that there exist vaguely formulated domestic laws governing surveillance operations. Vague or overbroad frameworks are prone to highly subjective interpretation and tend to invest excessive discretion in government authorities to take action against online freedom of expression. Therefore, companies must carefully examine the legal frameworks of the Government end-user to ensure that the laws do not permit arbitrary interference or attacks. Companies should also ensure that there exists independent and impartial judicial authority reviewing government-issued order for any surveillance operation.

In addition, Government end-users should provide companies with adequate explanation of the precise nature of the threat it intends to address with the surveillance technology. Therefore, in conducting due diligence, companies must determine whether the Government end-user has met its burden of establishing a "direct and immediate connection between the expression and the threat." A restriction must be more than merely useful, reasonable or desirable. It is also well established that necessity requires an assessment of proportionality.[5] Proportionality requires demonstrating that restrictive measures are the least intrusive instrument among those which might achieve their protective function and proportionate to the interest to be protected.[6]

Because of the highly advanced and versatile nature of technologies that are currently on the market and their intended and unintended impacts on human rights, due diligence efforts should not stop at the point of sales but must continue throughout the duration of the service or the product's life cycle. Furthermore, as correctly identified in the draft Guidance, the review of legal frameworks and practices of potential government end-users companies should accompany other safeguards including, but not limited to, 'privacy by design' features, regular programs of audits and human rights verification processes, and technical design features to flag, prevent or mitigate misuse.

III. Public Reporting and Transparency

The draft Guidance would recommend that companies publicly report a number of steps, including their human rights due diligence efforts, complaints processes, and general human rights policies. This would be in keeping with the UN Guiding Principles, which calls upon businesses to report on how they would address risks of human rights impacts.[7] The UN Guiding Principles emphasize that transparency takes "a variety of forms, including in-person meetings, online dialogues, consultation with affected stakeholders, and formal public reports."[8]

I commend the effort to highlight the importance of increasing transparency and accountability across the industry, as I believe that they are key elements in obtaining the

[5] Kaye, *supra* note 4, ¶ 35
[6] U.N. Human Rights Committee, General Comment No. 34 ¶ 34.
[7] UN GUIDING PRINCIPLES, Principle 21.
[8] *Id.*

goals of the draft Guidance. As discussed in my 2019 report, the private surveillance industry currently operates "under a cloak of secrecy"[9] with something close to impunity. Even though few companies have published their customer policies with some recognition of the need to respect human rights, the lack of insight into their standards and practices makes it difficult to evaluate how, if at all, such policies are actually being implemented.

I agree with the draft Guidance's position that due diligence processes must accompany mechanisms to increase public disclosure and accountability. As per the draft Guidance, companies must publicly report on their human rights policies, due diligence mechanism, and their review of complaints of misuse. The disclosures should include detailed information on the potential uses and capabilities of their products, the types of after-sales support provided, data concerning the number and type of sales to law enforcement, intelligence or other Government agencies or their agents, and any incidents of misuse. Furthermore, when companies detect misuses of their products and services to commit human rights abuses, they should promptly notify the relevant domestic, regional or international oversight bodies.

Establishing channels of communications and inviting input from various stakeholders including affected rights holders, civil society groups and digital rights organizations about the ongoing or potential impacts of their products and services are also recommended. Industry participants should engage in dialogues regarding industry-wide operationalization of the UN Guiding Principles, with particular attention to transparency standards, human rights due diligence, and remediation mechanisms.

Public disclosures enable end-users and other relevant stakeholders – such as civil society, academics, and international organizations – to discern how the companies' policies are being implemented, and provide the public with information necessary to raise public awareness, seek redress, or challenge any particular uses where appropriate. Therefore, private companies operating in the surveillance industry must subject themselves to robust transparency reporting of their business activities and their impacts on human rights to give meaning to their human rights policies.

IV. Grievance Mechanisms

The draft Guidance provides that companies should mitigate human rights risks through "contractual and procedural safeguards, and strong grievance mechanisms." In particular, with respect to grievance mechanisms, the draft Guidance recommends "secure, accessible, and responsive communications channels" and protection for both internal and external actors reporting misuse, as well as a formal follow-up mechanism.

One of the three pillars of the Guiding Principles is "greater access by victims to effective remedy, both judicial and non-judicial." Effective grievance mechanism is key in establishing sector-wide accountability, redressing victims for the harms, and assuming responsibility for the role private companies play in shaping privacy and freedom of

[9] Kaye, *supra* note 1, ¶ 29.

expression. Therefore, I am glad to see the Department's draft recommendation for establishing an effective grievance mechanism through measures including channels of communication, protection for internal and external whistleblowers, and timely follow-ups. In line with these recommendations, I also suggest additional measures that would help complainants seek compensation, apologies and other forms of redress, as appropriate. The effectiveness of a grievance mechanism will depend on its ability to assess the complaints independently and comprehensively, i.e. the ability of the adjudicating body to investigate the allegations of misuse and make decisions independently from the company's management. Furthermore, companies must enable actual, prompt, and meaningful reparation including restitution, compensation, rehabilitation, satisfaction and guarantees of non-repetition to the victims. Finally, new company policies on grievance mechanism should demonstrate willingness and concrete plans to investigate and remedy past violations.

V. Co-regulatory Initiatives

Addressing the global problem of targeted surveillance will require much more than policy implementations and initiatives by the private companies. Reports on misuses and serious human rights violations have demonstrated that self-regulation paradigm is insufficient to achieve human rights accountability in the industry. I therefore concluded in my 2019 report that effective governance requires inputs from civil society actors including activist, technologists, academics, and victims, as well as meaningful participation from State actors. This co-regulatory governance may provide a blueprint for human rights accountability in the private surveillance industry. In particular, co-regulatory initiatives developed to instill 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 (as your draft Guidance suggests) 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.[10]

In view of the above comments, I encourage the U.S. Government to take all steps necessary, including incorporating the recommendations of this communication, to provide a comprehensive guidance for the exporters of technologies with surveillance capabilities to mitigate adverse human rights impacts of their products. Furthermore, I urge you to consider integrating the human rights principles in new export controls, such as the upcoming controls of advanced surveillance technologies as part of BIS's review of emerging technologies.

Finally, I would like to inform you that this communication, as a comment on pending or recently adopted legislation, regulations or policies, and any response received will be made public via the communications reporting website within 48 hours. They will

[10] See Kaye, *supra* note 1, ¶¶ 61-64.

also subsequently be made available in the usual report to be presented to the Human Rights Council.

Please accept the assurances of my highest consideration.

David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression