MARCH 1, 2019

Global Justice Clinic

nyu school of law

# ATTEMPED DIGITAL SURVEILLANCE AS A COMPLETED HUMAN RIGHTS VIOLATION:

## WHY TARGETING HUMAN RIGHTS DEFENDERS INFRINGES ON RIGHTS

SUBMISSION TO THE UNITED NATIONS SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION

## SUMMARY

**The Global Justice Clinic ("GJC") at New York University School of Law[1] engages in work to prevent, challenge and redress rights violations related to global inequality. GJC's research on digital surveillance has uncovered a gap regarding the application of the international human rights law framework to *attempted* digital surveillance of human rights defenders, as opposed to *completed* surveillance. Attempted digital surveillance of a human rights defender is evidence of the unlawful targeting of that individual on the basis of their opinion. It not only gives the targeted individual a reasonable basis to fear that they are subject to surveillance; it also provides notice that existing due diligence frameworks, export control regimes, and other regulatory measures have failed to protect against human rights violations. Thus, when attempts to infect human rights defenders' digital devices with commercial spyware are discovered, the targeted individuals should have the opportunity to seek protection and remedy, and such instances should prompt governments and companies to strengthen the safeguards against such abusive conduct.**

**GJC makes this submission to underscore the need for further guidance on the prevention and remediation of such infringements of the rights to privacy and freedom of opinion and expression, and to encourage the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression ("Special Rapporteur") to address these issues in his report on commercial spyware.**

[1] This report does not purport to represent the institutional views, if any, of New York University. The report was authored by law student advocates in the Global Justice Clinic, Rashmika Nedungadi and Julie Bloch, under the supervision of Professor Margaret Satterthwaite and Nikki Reisch.

# I. Introduction

Targeting human rights defenders for digital surveillance because of the opinions they hold or the work they do is never permissible under human rights law. It infringes on the right to privacy, and chills the exercise of freedom of opinion and expression, regardless of whether the data or communications of the targeted individual are in fact intercepted. It is often hard to prove that such surveillance is occurring, that a digital device has been infected or personal data compromised. When evidence of an attempted infection with commercial surveillance software[2] or "spyware" comes to light, it not only puts the targeted human rights defender on notice that they may be subject to surveillance now or in the future, it also should put governments and companies on notice that their due diligence measures and regulatory protections are inadequate. Evidence of attempted infection of a human rights defender's digital device signals that there have been failures on the part of the company that supplies the software, as well as the governments of the home state where that company is based and the host state where the surveillance occurs, to refrain from and protect against such unlawful infringements of rights by: (1) ensuring that there is an adequate legal framework for authorizing any such targeting, subject to independent judicial review; (2) enacting and enforcing export control laws that prevent the sale of malicious software and other forms of digital weapons to governments that lack such minimal legal protections in their domestic laws; and (3) undertaking robust due diligence to ensure, at a minimum, that government purchasers of such software have those basic legal protections in place, furnish a legal basis for targeting any given individual with surveillance software, and afford individuals procedural protections against wrongful targeting.

As human rights defenders become more aware of the use of malicious surveillance software, they have become savvy in defending against its deployment, resulting in increasing numbers of known cases of attempted—but not completed—infection. From 2016 to 2018, the Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy at the University of Toronto, documented multiple infections and attempted infections of the digital devices of human rights advocates, political dissidents and journalists who had been publicly critical of the Mexican government's policies.[3] In early 2018, Pakistani human rights activist Diep Saeeda received a number of malicious messages sent to her Facebook and e-mail accounts. The content of the messages indicated that Saeeda was targeted based on her work as a

[2] "Commercial Surveillance Software" refers to technology created by private companies and sold commercially that is used to monitor digital activities. *See generally* Int'l Fed'n for Human Rights, *Surveillance Technologies: "Made in Europe"* (Dec. 2014), https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe.pdf; Citizen Lab, *Detekt spyware Detection Tool Released* (Nov. 24, 2014), https://citizenlab.ca/2014/11/detekt-spyware-detection-tool/; Privacy Int'l, *Explained: Our Criminal Complaint on Behalf of Tadesse Kersmo* (Feb. 20, 2014), https://privacyinternational.org/blog/1210/explained-our-criminal-complaint-behalf-tadesse-kersmo.

[3] Citizen Lab, *Reckless VI* (Nov. 27, 2018), https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/.

human rights activist.[4] In August 2018, an Amnesty International staffer received a malicious message containing a link to the "Pegasus" spyware platform[5] with a targeted message about their work in Saudi Arabia. These attempted infections represent only a fraction of the instances—known and unknown—in which human rights defenders have been subjected to targeted surveillance. In each case, the attempt to infect the human rights defenders' devices was evidence of unlawful targeting. Although the surveillance attempt may have been incomplete, the targeting was carried out, and in itself had adverse impacts on the individual defenders and their work. In light of these developments, there is a need to: clarify how international human rights law applies to attempted surveillance of human rights defenders; recognize and document the human rights harm such attempts cause; and strengthen the safeguards in place to prevent and respond to such attempts, thereby reducing the risk of completed unlawful surveillance.

The use or attempted use of commercial surveillance software to infect the digital devices of human rights defenders in order to access their personal data and communications infringes the rights to privacy, freedom of opinion, and freedom of expression, as it involves an intentional invasion of privacy based on opinion. While the primary actor in such cases is usually a government agency, the surveillance industry, comprised of the companies that develop, market and deploy digital surveillance technologies, enables these international human rights violations. States where surveillance companies are domiciled ("home states"), as well as the states that purchase and employ the companies' technologies ("host states"), have a duty to uphold the provisions of human rights law, such as the International Covenant on Civil and Political Rights ("ICCPR" or "the Covenant"). Under Article 2(1) of the ICCPR, states are required not only to refrain from violating Covenant rights, but to protect individuals against violations by private third parties, including by spyware companies, which take place on their territory or under their jurisdiction.[6]

Home states violate their duty to protect when they fail to prevent conduct by spyware companies that foreseeably results in the violation of human rights defenders' rights under Articles

[4] Amnesty Int'l, *Human Rights under Surveillance: Digital Threats Against Human Rights Defenders in Pakistan*, at 15, AI Index ASA 33/8366/2018 (2018) [hereinafter *Human Rights under Surveillance*].
[5] Pegasus is a form of malware, developed by the Israeli firm NSO, that infects mobile devices through specially-crafted "exploit links." Citizen Lab, *Hide and Seek* (Sept. 18, 2018), https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.
[6] International Covenant on Civil and Political Rights art. 2(1), Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]. *See* Human Rights Comm., General Comment 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, ¶ 8, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004) [Hereinafter General Comment 31]. *See also* Doe v. Fed. Dem. Rep. of Ethiopia, Brief of Amici Curiae United Nations Human Rights Experts in Support of Plaintiff-Appellant and Reversal, 2016 WL 6476760, 6–8 (C.A.D.C. 2016); U.N. Human Rights Office of the High Comm'r, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, Foundational Principles (2011), https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf [hereinafter Guiding Principles].

17 and 19—whether at home or abroad.[7] Given that the unlawful surveillance of a human rights defender abroad may be facilitated or effectuated by a spyware company at home, the home state has a duty to take affirmative steps to screen for and prevent such risks, through steps such as restricting the sale of spyware products to states known to abuse human rights.[8] The duty to protect also entails a due diligence obligation: state parties are responsible for ensuring that businesses within their jurisdiction exercise due diligence to prevent their entities or agents from violating, or causing or contributing to the violation of, Covenant rights.[9]

This submission argues that attempted digital surveillance of human rights defenders, like completed surveillance, constitutes unlawful targeting of individuals on the basis of their opinion. Such abusive conduct results from the failures of corporations to avoid causing or contributing to such violations, and the failures of states to respect Covenant rights in their own practice and to protect individuals against violations by private actors. The submission concludes with recommendations to the Special Rapporteur about the need to clarify how the existing legal framework applies to attempted digital surveillance, and what the legal framework requires of states and corporate actors in the surveillance industry.

Throughout this submission, we use the terms "targeted digital surveillance" and "human rights defenders" to set out the applicable legal framework. For the purposes of this submission, "targeted digital surveillance" refers to the use of surveillance technology against specific individuals over digital channels, such as mobile messaging applications and email. The term "human rights defenders" refers to human rights activists, political dissidents, and journalists—broadly speaking, individuals who work toward the promotion and protection of human rights,[10] and who, as a result of their work are frequently the targets of repression by states and private groups.[11] While this submission focuses on human rights defenders, it should not be construed to endorse or condone targeted surveillance against others, or to suggest that the human rights violations involved in targeted digital surveillance are limited to human rights defenders.

---

[7] Econ. & Soc. Council, General Comment No. 24 on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities, ¶ 18, U.N. Doc. E/C.12/GC/24 (Aug. 10, 2017) [hereinafter General Comment No. 24]. *See also* Guiding Principles, *supra* note 6, at principle 3 and commentary.

[8] Rep. of the Office of the U.N. High Comm'r for Human Rights, The Right to Privacy in the Digital Age, ¶ 34, U.N. Doc. A/HRC/27/37 (June 30, 2014) [hereinafter The Right to Privacy in the Digital Age]; General Comment No. 24, *supra* note 7, ¶ 18–19.

[9] Guiding Principles, *supra* note 6, at principles 15 and 17. *See also* Econ. & Soc. Council, General Comment No. 20: Non-Discrimination in Economic, Social and Cultural Rights (art. 2, para. 2, of the International Covenant on Economic, Social and Cultural Rights, ¶ 16, U.N. Doc. E/C.12/GC/24 (July 2, 2009).

[10] U.N. Office of the High Comm'r on Human Rights, *Who is a Defender?*, https://www.ohchr.org/en/issues/srhrdefenders/pages/defender.aspx (last accessed Mar. 1, 2019).

[11] Int'l Fed'n for Human Rights, *Human Rights Defenders*, https://www.fidh.org/en/issues/human-rights-defenders/ (last accessed Mar. 1, 2019).

# II. International bodies should recognize that attempted surveillance of human rights defenders violates Article 17 of the ICCPR, regardless of whether an infection occurs.

## A. The *attempted* digital surveillance of a human rights defender constitutes an *actual* or *completed* interference with a recognized zone of privacy, because it generates a reasonable fear that the target has been or will be the subject of surveillance.

To constitute an invasion of privacy under Article 17 of the ICCPR, conduct must involve an "interference" with a recognized "zone of privacy." Digital information and communications are recognized to fall within zones of privacy under Article 17.[12] "Interference" in the surveillance context is defined as "the collection and retention of communications data…whether or not those data are subsequently consulted or used."[13] However, General Comment 16 to ICCPR Article 17 also recognizes that "the mere *possibility* of communications information being captured creates an interference with privacy."[14]

Deploying a malicious message or call is sufficient to manifest not just the "mere *possibility*" but the reasonable likelihood of a state conducting surveillance, and the reasonable likelihood that the state has already succeeded in collecting private data through a different digital platform. Delivering an infected link to the device of a targeted human rights defender through a call, text or e-mail is sufficient conduct to constitute an interference with the right to privacy, even if the target did not activate the link and no digital communications were accessed, because it generates reasonable fear that the person is now or will in the future be subject to surveillance. The targeting of an Amnesty International staff member in June 2018 serves as an example of such interference. The Amnesty staff member received a suspicious WhatsApp message with Saudi-Arabia related content that if clicked, would have infected the device with the Pegasus spyware system.[15] By alerting the target to the existence of an immediate surveillance threat,[16] the attempted deployment of spyware against the Amnesty staff member interfered with their privacy.

The sense of fear or uncertainty about "being watched" that follows an attempted spyware infection is comparable to the fear generated by mass surveillance programs, which have been widely condemned. The fear created by such programs along with the constant threat created by

---

[12] Human Rights Comm., General Comment No. 16: Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation), ¶ 10, U.N. Doc. HRI/GEN/1/Rec.9 (Vol. I) (Apr. 8, 1998) [hereinafter General Comment No. 16].
[13] The Right to Privacy in the Digital Age, *supra* note 8, ¶ 20.
[14] *Id.*
[15] Amnesty Int'l, *Meet NSO: a go-to group for human rights abusers* (Aug. 6, 2018), https://www.amnesty.org/en/latest/news/2018/08/is-nso-group-a-goto-company-for-human-rights-abusers/.
[16] The Right to Privacy in the Digital Age, *supra* note 8, ¶ 20.

the very existence of such widespread surveillance interferes with the privacy of the population the program is deployed.[17] As stated by the European Court of Justice, "the fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance."[18] A comparable fear exists for a human rights defender after an attempted surveillance attack; indeed, the effect is likely—and justifiably—more severe given the personal nature of the targeting. Recent examples of targeting, such as the repeated malicious messages sent to both Andres Villarreal and Ismael Bojorquez by the Mexican government-linked Pegasus operator,[19] indicate that an attempted digital surveillance attack is likely to involve the systematic targeting and harassment of a human rights defender until an attempt to collect communications data is successful.

The existence of so-called "zero-click" technology, an infection method reportedly developed by spyware companies such as NSO Group, heightens the sense of vulnerability and uncertainty around whether a human rights defender who was the target of an attempted infection is being surveilled. Zero-click involves an operator sending malware through SMS messaging, but does not require a target to click on any URL link for the spyware to remotely install and collect data.[20] The existence of zero-click means that human rights defenders can "never know for certain if they are being targeted or have unwittingly downloaded some kind of spyware."[21] Diep Saeeda, a Pakistani activist who was a victim of attempted targeted surveillance, has explained how this constant uncertainty results in a climate of repression for human rights defenders: "every time I open an email I am now scared."[22]

Moreover, the conduct necessary to attempt to infect the digital device of a targeted human rights defender with surveillance software satisfies the elements of "attempt" as it is commonly understood in the criminal context in jurisdictions around the world. Under various common and civil law constructions, attempt involves the intent to commit an offense as well as substantial steps towards the commission of the crime. [23] Once an agent has sent a malicious link, the success

---

[17] *Id.*
[18] Case C-203/15 [2016] *Tele 2 Sverige AB v. Swedish Post and Telecom Authority,* ECR.
[19] Citizen Lab, *Reckless VI* (Nov. 27, 2018), https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/.
[20] Citizen Lab, *The Million Dollar Dissident* (Aug. 24, 2016), https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.
[21] *Human Rights Under Surveillance*, *supra* note 4, at 15.
[22] *Id.*
[23] American Law Institute, *Model Penal Code* §5.01(1)(c)(1962); Criminal Attempts Act 1981, c.47, s.1 (United Kingdom); Criminal Law of the People's Republic of China, Art. 23(2) (1979); Art. 121-5, *Code penal* (France); C.XXIII, s. 511, IPC (India); Keiho, C. VIII, Art. 43 (Japan) (Some jurisdictions vary their definition on the amount of preparatory conduct needed to constitute an attempt. For example, the United Kingdom punishes "an act which is more than merely preparatory" whereas the United States requires that an offender is "dangerously close to carrying out a criminal act." Several jurisdictions also conclude that an attempt has occurred where the requisite intent exists, and where the offender is only prevented from committing the crime due to circumstances out of their control).

or failure of the infection is out of their hands, and is solely dependent on whether the target clicks the link.[24] Analogizing from concepts of criminal attempt, it is logical that if the surveilling agent has taken the steps required to effectuate a violation, and the only remaining step to complete the violation is an action by the victim, then agent has committed the violation.

### B. Attempted surveillance of human rights defenders is unlawful when it lacks a domestic legal basis and prior judicial authorization.

The purpose behind installing malicious software on an individual's digital device is the same whether the infection is successful or not: to surveil the individual. Thus, determining whether completed or attempted surveillance is unlawful or arbitrary involves the same analysis.

Surveillance must be governed by a clearly defined legal regime subject to independent judicial oversight. As an invasion of privacy, targeted surveillance may be lawful only if properly authorized by domestic legislation. For a surveillance law to be permissible under international human rights law, it must be "publicly accessible," "tailored to specific aims," "sufficiently precise, specifying…the categories of persons who may be placed under surveillance," and it must "provide effective safeguards against abuse."[25] Furthermore, any invasion of privacy must be authorized by an independent judiciary on a case-by-case basis.[26]

There is no indication, in any of the countries implicated in the case studies cited above (Mexico, Pakistan or Saudi Arabia) that judicial authorization was sought, let alone obtained, prior to the deployment of a malicious message. As made clear under the ICCPR, judicial authorization is *required* for each case of infringement on the right to privacy.

[24] The intent to surveil is clear from the fact that a malicious message was sent with a link to malware. The "acts" leading up to completed surveillance (successful infection) include identifying a specific individual, collecting and verifying an individual's phone number or e-mail account, performing research on the target's interests to craft a sufficiently baiting message, deploying a malicious message, and waiting for the target to click the link. But after the link is deployed, there are no further steps to be completed apart from those taken by the targeted individual. Where zero-click is used, there are *no* additional steps. *See* Citizen Lab, *The Million Dollar Dissident* (Aug. 24, 2016), https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

[25] The Right to Privacy in the Digital Age, *supra* note 8, ¶ 28. *See also* Malone v. United Kingdom (No. 8691/79) Eur. Ct. H.R., Judgment, ¶ 68 (Aug. 2, 1984) (all applications of targeted digital surveillance would need to sufficiently indicate the *scope* of applicable national law in order to protect the individual against arbitrary interference).

[26] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Human Rights Council, ¶ 54, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013) (by Frank La Rue) [hereinafter La Rue]; General Comment No. 16, *supra* note 12, ¶ 8.

### C. Digital surveillance of human rights defenders constitutes an arbitrary interference as it is not necessary or proportionate to a legitimate government aim.

Even when the legal regime authorizing surveillance is sufficiently clear, it may still be arbitrary if it is not necessary and proportional to a legitimate aim.[27] To establish the "necessity" justifying digital surveillance, states frequently invoke a national security exception, which is one of a limited number of recognized exceptions to the right to privacy.[28] International law may permit limited surveillance activity as "necessary in a democratic society,"[29] confined to the context of investigation and law enforcement activity related to crime and terrorism. The onus of establishing that the surveillance is necessary, however, falls on the state, which has a burden to show the nature of the national security threat posed by *each* individual surveilled—not simply that a surveillance capability or program is legitimate in the abstract.[30] In practice, states have not argued that targeted surveillance of human rights defenders is necessary for or proportional to national security or crime prevention.[31] Nor could they: regardless of state justifications, human rights defenders may *never* be subject to surveillance solely on the basis of their opinion, their status as human rights defenders, or on the basis of their work. Although states may argue that surveillance is necessary for national security purposes, monitoring, intimidating or otherwise interfering with the activities of individuals because they are critical of the government is not a legitimate aim warranting infringement.

Even if a legitimate aim existed, surveilling human rights defenders would never be proportionate to legitimate aims. Under the principle of proportionality, information accessed must be confined to that which is relevant and material to a serious crime or specific threat to a legitimate

---

[27] *See* The Right to Privacy in the Digital Age, *supra* note 8, ¶ 22–23; Human Rights Comm., General Comment No. 34: Article 19: Freedoms of opinion and expression, ¶ 23, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011) [hereinafter General Comment No. 34]. *See also* Doe v. Fed. Dem. Rep. of Ethiopia, Brief of Amici Curiae United Nations Human Rights Experts in Support of the Plaintiff Appellant and Reversal, 2016 WL 647670, para. 14 (C.A.D.C. 2016).

[28] Interpretive instruments to Article 17 have indicated that the exceptions applicable to Article 19 are equally applicable to Article 17, therefore legitimate government aims for surveillance would include limitations for the "respect of the rights or reputations of others" and the "protection of national security…public order…[or] public health or morals. *See* ICCPR, *supra* note 6, at art. 19(3); Rep. of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Human Rights Council, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009) (Martin Scheinin) [hereinafter Scheinin].

[29] *See* Weber & Saravia v. Germany (No. 54934/00), 2006-XI Eur. Ct. H. R. 1173, ¶ 105.

[30] *See, e.g.*, Human Rights Comm., Communication No. 926/2000, *Shin v. Republic of Korea*, ¶ 7.2, U.N. Doc. CCPR/C/80/D/926/2000 (Mar. 16, 2004) ("the State party must demonstrate in a specific fashion the precise nature of the threat to any of the enumerated purposes caused by the author's conduct").

[31] *See* Azam Ahmed, *Mexican President Says Government Acquired Spyware but He Denies Misuse*, N.Y. TIMES (June 22, 2017), https://www.nytimes.com/2017/06/22/world/americas/mexico-pena-nieto-hacking-pegasus.html; Citizen Lab, *Bittersweet* (Feb. 11, 2017), https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/ ("the targets of Bitter Sweet operations have not been accused by anyone of being criminals or terrorists").

aim alleged.[32] The intrusion that the installation of spyware entails – allowing the surveilling government unrestricted access to all data—is too broad and nearly impossible to justify as necessary to a legitimate aim, except perhaps in the most extreme and heightened cases of national security. Citizen Lab investigations into the targeting of human rights defenders with Pegasus,[33] malware produced by the Israeli spyware firm NSO Group, have revealed how invasive it is: the software effectively turns "the [infected] device into a silent digital spy,"[34] allowing operators to capture files, messages, location, and to actively and passively record through the phone's microphone and video camera, and more.

# III. Attempted surveillance of human rights defenders violates both freedom of opinion and freedom of expression under ICCPR Article 19 because, like completed surveillance, it targets individuals based on their opinion, and results in a chilling effect that suppresses human rights defenders' communicative activities.

## A. Because targeting is based on opinion, attempted digital surveillance of human rights defenders violates freedom of opinion, a non-derogable right.

ICCPR Article 19 defines the freedom of opinion as the right to hold opinions without interference. Unlike the right to privacy, the freedom of opinion is a non-derogable right, and does not allow for exceptions in any cases—including national security. Successfully installing surveillance software on an individual's device and monitoring their activity constitutes an interference with one's freedom of opinion, as it chills one's ability to hold an opinion without fear of interference. Attempted surveillance of human rights defenders likewise infringes on the right to hold an opinion. *Any form of effort* to coerce an individual to hold or not hold any opinion is prohibited,[35] making the very targeting of a human rights defender based on their opinion a

[32] Article 19 et al., *International Principles on the Application of Human Rights to Communications Surveillance*, at 8 (May 2014), https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf.
[33] *See, e.g.*, Citizen Lab*, The Million Dollar Dissident* (Aug. 24, 2016), https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; Citizen Lab, *Reckless VI* (Nov. 27, 2018), https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/.
[34] Citizen Lab*, The Million Dollar Dissident* (Aug. 24, 2016), https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.
[35] General Comment No. 34, *supra* note 27, ¶ 10 (citing Communication no. 878/1999*,* Kang v. Rep. of Korea (15 Jul. 2003)) (emphasis added).

violation of their freedom of opinion.[36] Because human rights defenders are subject to targeting specifically because of their opinion, both actual and attempted surveillance is unlawful as it plainly demonstrates an effort to suppress or limit human rights defenders' opinions.

### B. The chilling effect on communications produced by attempted digital surveillance violates the freedom of expression.

Freedom of expression is essential to the work of human rights defenders. Through public communications—including digital writings, images, and social media commentary—human rights defenders are able to inform and empower society; and through private communications—including emails, messaging, and voice calls—human rights defenders are able to collaborate, conduct investigations, and keep abreast of developments in human rights. Both spheres of expression are put at risk through targeted surveillance.

Digital surveillance—and the threat of digital surveillance—has a "chilling effect" on both private and public forms of expression, directly reducing advocates' ability to perform their work effectively. This effect also inhibits the "freedom to seek, receive and impart information and ideas of all kinds" guaranteed under Article 19(3) of the ICCPR. The targeted surveillance of human rights defenders can threaten, discredit or intimidate them.[37] Fear of government retaliation contributes to a "climate of repression" and can result in human rights defenders being unable to complete their work.[38] The "mere existence" of surveillance programs—and especially targeted surveillance programs—creates an indirect limitation that has a chilling effect on the right to freedom of expression.[39]

The freedom of expression may be restricted, where restrictions are provided by law and necessary for the respect of the rights of others, or for the protection of public order or of public health or morals. Freedom of expression can be infringed upon—in limited situations—for national security purposes. When invoking a national security exception, however, a state party must demonstrate the direct and immediate connection between the expression and the threat.[40]

Such an immediate connection is absent when the government engages in surveillance tactics designed to frighten critics into silence. For example, government-linked Pegasus operators targeted two directors of Mexican NGOs while the NGOs were campaigning to increase the soda tax rate in Mexico and raise awareness of the health risks associated with sugary drinks.[41] The

[36] *See, e.g.*, Citizen Lab, *Bittersweet* (Feb. 11, 2017), https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.
[37] *See Human Rights under Surveillance*, *supra* note 4.
[38] *Id.*; Citizen Lab, *Bitter Sweet* (Feb. 11, 2017), https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.
[39] The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet, ¶ 150, Doc. No. OEA/Ser.L/V/II, CIDH/RELE/INF. 11/13 (Dec. 31, 2013).
[40] General Comment No. 34, *supra* note 27, ¶ 35.
[41] Citizen Lab, *Bitter Sweet* (Feb. 11, 2017), https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.

targeting took place as the soda industry was exerting significant political pressure on the Mexican government.[42] Similarly, Claudio X. Gonzalez, the director of a prominent Mexican anti-corruption organization, was targeted after reporting on a presidential scandal.[43] Targeting of human rights defenders so all to chill all their expressive conduct or silence those reporting on facts adverse to government positions[44] is not a legitimate government objective.

## IV. Appropriate remedies must be available for any attempted surveillance.

ICCPR Article 2 provides that there must be an effective remedy available for violations of Covenant rights.[45] The forms that such remedy may take involve not only reparation and satisfaction, but—of particular importance in the context of digital surveillance—guarantees of non-recurrence. Recognizing that an attempted digital infection of a human rights defender is evidence of a completed violation—the unlawful targeting of that individual on the basis of opinion—should give rise to certain remedial measures both at the individual and the institutional level. Attempted infection puts states and commercial spyware companies on notice that they need to strengthen their due diligence systems and regulatory framework to prevent the wrongful deployment of surveillance software. Human rights defenders who are victims of attempted infection should have some recourse or means to alert authorities or appropriate bodies to the attack and trigger remedial measures.

The harm that an individual incurs as a result of an attempted digital infection is often difficult to quantify; as discussed above, it involves fear, uncertainty and actions not taken. However, it often also involves an intense chilling effect and the pecuniary harms that accompany the purchase of new phones, adoption of alternative communication techniques, and even physical relocation. In terms of freedom of expression and freedom of opinion, pecuniary harms are more quantifiable, as a chilling effect can result in human rights defenders' putting a halt to their work entirely, minimizing their involvement in the work, refraining from publication of their opinions, and more. Given the challenges of assessing the harms resulting from attempted surveillance and crafting appropriate forward-looking (preventive) as well as compensatory remedies, there is a need for greater attention to these issues and guidance from international human rights bodies such as the Special Rapporteur.

[42] *Id.*
[43] Citizen Lab, *Reckless V* (Aug. 30, 2017), https://citizenlab.ca/2017/08/nso-spyware-mexico-corruption/.
[44] *See Human Rights under Surveillance*, *supra* note 4.
[45] ICCPR, *supra* note 6, at art. 2(3)(a).

# V. Recommendations: Clarify the legal standard concerning attempted digital surveillance and the duties of companies and home states.

Clarification by the Special Rapporteur of the legal framework protecting human rights defenders from both attempted and completed targeted surveillance would significantly advance efforts to ensure defenders can enjoy their Covenant rights. Strong articulation of the due diligence obligations of surveillance software companies, the steps that states must take to regulate and monitor their activities, as well as the measures needed to ensure defenders can access remedies for targeted surveillance attacks would be very valuable. GJC respectfully offers the following recommendations for consideration by the Mandate:

1. **Call upon states to actively regulate and monitor surveillance software companies domiciled in their territory to ensure that sale of any surveillance software complies with Article 17 and 19, and that any misuses of the software against human rights defenders are remedied. This could include, for example, passing stricter export laws and regulations, effectively monitoring compliance with such standards, and sanctioning companies when they fail to comply. To obtain export licenses, companies should at a minimum be required to demonstrate that they have put in place effective mechanisms to protect the rights of human rights defenders.**

    - States must ensure that export control regimes are sufficiently robust to prevent use of exported spyware against human rights defenders, and to withdraw licenses upon credible reports of abuse. Agencies responsible for licensing must have adequate funding and technical capacity to review surveillance programs, safeguards, and mechanisms for preventing abuse.

        - States should prohibit companies from selling to countries with non-existent or inadequate legal frameworks and regulations.

    - States should require companies to establish effective mechanisms to prevent the use of their products in the targeted surveillance of human rights defenders. These mechanisms could include, for example, establishing Business and Human Rights Committees responsible for exercising due diligence before any sales. Such Committees should adhere to regular reporting standards, such as a requirement to meet regularly and send reports to the state detailing how the company is respecting its human rights obligations.

2. **Call upon companies that produce or employ targeted surveillance tools to perform robust and effective due diligence on all sales of surveillance equipment to ensure that governments are not targeting human rights defenders using their tools.**

    - Surveillance software companies must ensure that a state purchasing surveillance software can satisfy the principles of legality, proportionality and necessity in its use. In doing so, companies must review the proposed buyer's legal framework, history of abuse, and mechanisms for judicial control of surveillance operations, and must refuse to sell to countries with a history of abuse—especially past targeting of human rights defenders.

    - Review the legal framework to ensure it provides mechanisms for redress, including remedy and judicial review, in cases of wrongful attempted or completed targeted surveillance.

    - Ensure that, to the extent companies are involved in specific individual cases, the purchasing country has provided proof of judicial authorization for the surveillance of each specific person. To the extent such authorization is missing, mandate that the company must refuse to allow the use of such software.

3. **Call upon companies to refuse to sell to countries that - either in their legal framework or in publicly-reported practice - include human rights defenders as legitimate targets of surveillance or have a history of targeting—for surveillance, harassment, imprisonment, or other human rights violations—human rights defenders.**

4. **Call upon states to make available appropriate remedies for both completed and attempted surveillance of human rights defenders resulting from the sale of surveillance software by companies based within their jurisdiction.**

    - Review and enact, where necessary, reforms to legal frameworks, rules concerning standing and extraterritoriality, classified information, and national security exceptions to ensure that human rights defenders may successfully pursue remedies in countries where surveillance software companies are domiciled.

- Recognize the full panoply of harms entailed in targeting and attempted surveillance of human rights defenders.