Clipping Pegasus's Wings

#2 Pegasus's impact on human rights

THE PRESENT LEGAL LANDSCAPE FOR RESTRAINING THE PRIVATE SURVEILLANCE INDUSTRY'S GLOBAL ATTACK ON HUMAN RIGHTS & A ROADMAP TO A BAN

by International Justice Clinic of University of California, Irvine School of Law

#2 Pegasus's impact on human rights

International human rights law provides for a framework of protections and guarantees of fundamental human rights according to which any state conducts, including use of surveillance technologies must be assessed. In the context of surveillance, the most relevant instrument in international human rights law is International Covenant on Civil and Political Rights (ICCPR), which protects the right to privacy in Article 17 and the right to freedom of opinion and expression in Article 19.

The global proliferation of spyware highlights the importance of international human rights law, which provides a legal framework for the fight against its use. Further, given that international human rights law has significantly developed over the course of years—through the adoption of nine international human rights treaties and treaty bodies' interpretations, etc.—human rights law serves as a useful tool to gauge the impact of spyware on individuals and society and consider necessary regulations. The accretion of norms helps us understand and address emerging human rights issues caused by digital surveillance.

A. PRIVACY AND FREEDOM OF EXPRESSION, AMONG OTHER FUNDAMENTAL HUMAN RIGHTS

Article 17(1) of the ICCPR guarantees that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence." "Privacy" includes informational privacy, namely, "the ability of individuals to determine who holds information about them and how that information is used."[1] The possibility of a spyware infection

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (April 17, 2013), A/HRC/23/40, para. 22.

undermines an individual's ability to control their personal information and communication, thus interfering with their right to privacy.[2]

Article 19(1) guarantees the right to maintain opinions without interference, and as such, it permits no exception or restriction. Article 19(2) guarantees the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers [...]." The right to freedom of expression is essential for both human dignity and democratic self-governance.[3] Spyware interferes with the rights to freedom of opinion and expression as the actual and perceived imminent threat of retaliation incentivizes individuals, including those actually and potentially targeted, or incidentally surveilled, to self-censor, prevents them from imparting their expressions and ideas, and deprives them of the ability to freely conduct research online or contact informational sources. Altogether, it discourages individuals from seeking and receiving information (often referred to as a "chilling effect"). In the digital age, the right to privacy is a gateway to the exercise of the right to freedom of expression because the lack of sufficient privacy protection leads to the chilling effect, which interferes with the right to freedom of expression.

ICCPR Article 21 guarantees the right to peaceful assembly. By enabling individuals to express themselves collectively and to participate in shaping their societies, it serves both human dignity but also democracy. Spyware interferes with the right to peaceful assembly because, like the implication with the right to freedom of opinion and expression, individuals are dissuaded to prepare, organize, or participate protests online and offline if they know they are likely to be surveilled by the government.

B. THE STRICT CONDTIONS APPLIED TO PERMITTTED RESTRICTIONS OF FUNDAMENTAL HUMAN RIGHTS

The right to privacy and the right to freedom of expression allow for interference in exceptional cases where a state has shown that the prescribed conditions are met (see especially Article 19(3)). Notably, the possibility of restriction does not pertain to the right to freedom of opinion.

Broadly speaking, both Articles require the application of the so-called three-part test (which require "legality," "legitimacy," and "necessity and proportionality"). Given the interlocking nature of both rights in the context of surveillance, all the distinctive elements in the test must be met.[4]

---

[2] See Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age (August 3, 2018), A/HRC/39/29, para. 7, citing European Court of Human Rights, Roman Zakharov v. Russia, application No. 47143/06, judgment of December 4, 2015; and Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age (June 30, 2014), A/HRC/27/37, para. 20, citing European Court of Human Rights, Weber and Saravia v. Germany and Malone v. UK. See also, European Court of Human Rights, Klass v. Germany, para. 41.

[3] Human Rights Committee General Comment No. 34: Article19: Freedom of opinion and expression (September 12, 2011), CCPR/C/GC/34, para.2.

[4] See Surveillance and human rights, *supra* note 1, para. 24.

i. Legality

Legality includes two elements: first, the interference is provided by law, non-discriminatory, accessible, and specific enough to serve as an advance notice to individuals and as a limitation of a state's discretion (a state thus must, *prior to using spyware*, enact law that constrains the state's use of spyware in order to meet all required elements under the legality test); and second, it is accompanied by strict safeguards which sufficiently eliminate the risk of abuse of surveillance are in place, which we will further detail below.[5]

Given spyware's intrusiveness, it is highly questionable whether safeguards against abuse are practically possible. However, assuming otherwise, the safeguards required under the legality prong would need to include at least the following:

a. independent and impartial judicial pre-authorization of *all* cases of spyware use, regardless of domestic or extraterritorial use;[6]
b. effective and independent official oversight which (i) monitors every process of each spyware use, including judicial pre-authorization, actual spyware use, and termination of the use, (ii) investigates alleged misuse of spyware, and (iii) publicly discloses the result of such oversight for public scrutiny;[7]
c. prohibition of data sharing and data repurposing;[8]
d. prohibition of use of evidence which is directly or indirectly obtained through the misuse of spyware.[9]

ii. Legitimacy

Article 19(3) of the ICCPR identifies an exhaustive list of legitimate bases for a restriction on freedom of expression: the rights or reputations of others; national security; public order; public health or morals.[10] States must provide an "articulable and evidence-based

---

[5] See, id., paras. 23; Article 17(2) of the ICCPR; Human Rights Committee, *Madhewoo v Mauritius*, CCPR/C/131/D/3163/2018, paras. 7.4 and 7.6; Human Rights Committee, Concluding Observation on the United States of America (April 23, 2014), CCPR/C/USA/CO/4, para. 22. See also The right to privacy in the digital age, (2014), *supra* note 2, paras. 28 and 37.

[6] See Human Rights Committee, Concluding Observations on Italy (May 1, 2017), CCPR/C/ITA/CO/6, para. 37. See also, The right to privacy in the digital age (2018), *supra* note 2, para. 39 ([the judicial branch] "needs to make sure that there is clear evidence of a sufficient threat and that the surveillance proposed is targeted, strictly necessary, and proportionate and authorize (or reject) ex ante the surveillance measures;" The right to privacy in the digital age (2014), *supra* note 2, para. 30.

[7] See, for example, Human Rights Committee, Concluding Observations on Macao, China (July 27, 2022), CCPR/C/CHN-MAC/CO/2, para. 33; Human Rights Committee, Concluding Observations on Georgia (September 13, 2022), CCPR/C/GEO/CO/5, para. 40. See also, The right to privacy in the digital age (2018), *supra* note 2, paras. 39 and 40; The right to privacy in the digital age (2014), *supra* note 2, para. 37 and 38.

[8] See *Madhewoo v Mauritius*, *supra* note 5, paras. 7.4 and 7.6; Concluding Observations on Canada (August 13, 2015), CCPR/C/CAN/CO/6, "C. Counter-terrorism."

[9] See Human Rights Committee, General Comment No. 20: Article 7 (Prohibition of torture, or other cruel, inhumane or degrading treatment or punishment (10 March 1992), para. 12.

[10] General Comment 34, *supra* note 3, paras. 29-32.

justification for the interference," which includes the sufficient indications of specific national security harms.[11]

Silencing journalists, government critics, and human rights defenders itself could never be qualified as a legitimate purpose.[12] Notwithstanding assertions that Pegasus helps governments fight terrorism and solve crimes,[13] widespread reporting indicates that Pegasus has been used to target journalists, human rights defenders and activists.

Examples are legion suggesting that spyware is frequently deployed to surveil and silence human rights defenders, activists, opposition leaders, and journalists from cognizable social and political groups and those who belong to racial, religious, ethnic, national, or other minority communities. Such use of spyware just for the purpose of silencing critics would categorically fail to meet the legitimate test.

iii. Necessity and Proportionality

Article 19(3) requires that any restriction must be: (i) appropriate to achieve the legitimate purpose; (ii) the least restrictive among options which might achieve the purpose and must not be overbroad; and (iii) proportionate to the interest to be protected in a specific situation.[14] The test also requests "a detailed and evidence-based public justification."[15]

Spyware such as Pegasus allows indiscriminate and virtually (if not actually) complete access to data and recording functions on a target's mobile device, making it conceptually impossible to keep the privacy restriction to the extent "necessary" to achieve the legitimate aim. Such access lacks discrimination, the ability to distinguish between, for instance, warranted information-access and non-warranted. Intrusive spyware does not separate information relevant to a legitimate investigation from information outside the investigation's scope.[16]

Given its unrestrained access to data stored in or connected to the target's device, its use would by nature fail to meet the necessity requirement, meaning spyware inevitably allows a user to access data which is not necessary for a legitimate aim. As the UN Special Rapporteur on human rights and counter-terrorism has noted, "The fact that something is technically feasible, and that it may sometimes yield useful intelligence, does not by itself mean that it is either reasonable or lawful."[17] It follows that even if a portion of the data acquired on devices may inevitably be useful, the limitless breadth of information accumulated through the use of Pegasus would not be necessary.

---

[11] The report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (September 23, 2014), A/69/397, para. 12.
[12] General Comment 34, *supra* note 3, paras. 23.
[13] Cyber Intelligence For Global Security and Stability, NSO Group, https://www.nsogroup.com/.
[14] Id., paras. 33-36.
[15] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: The use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age (May 22, 2015), A/HRC/29/32, para. 35.
[16] David Pegg and Sam Cutler, What is Pegasus spyware and how does it hack phones?, The Guardian (July 18, 2021), https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones.
[17] The report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, *supra* note 11, para. 11.

In conclusion, under international human rights law, a strong case can be made that the use of spyware with equivalent characteristics as Pegasus cannot satisfy the requirements of Article 17(1)(2) and 19(2)(3).