UNIVERSITY OF CALIFORNIA, IRVINE
BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTACRUZ

Professor David A. Kaye
Clinical Professor of Law
Director, International Justice Clinic
UN Special Rapporteur on Freedom of Expression (2014-2020)

401 E. Peltason Dr., Ste. 3800-C
Irvine, CA 92697-8000
+1 949 824 2427
dkaye@law.uci.edu

July 26, 2023

The Honorable Palmer Gene Vance II
Chair of the House of Delegates
American Bar Association
321 North Clark Street
Chicago, IL 60654

RE: Proposed ABA resolution concerning commercial spyware

Dear Mr. Vance,

I am writing with respect to the proposed Resolution 508 of the ABA Section of Civil Rights and Social Justice, which calls for a moratorium on the sale, purchase, transfer, servicing, and use of commercial spyware until a robust international regulatory framework is put in place. The resolution, to be considered at the upcoming Annual Meeting, rests on the findings of a formidable report of the Section, not to mention on extensive testimony of victims and reporting of journalists, human rights organizations, regional organizations, and United Nations (UN) human rights bodies stretching back several years. As far back as 2019, as UN Special Rapporteur on the freedom of opinion and expression, I highlighted the grave human rights violations posed by targeted surveillance technologies operating in a globally lawless environment and called for actions to be taken to rein in the industry, including a moratorium as a critical step in rooting the rule of law and human rights compliance in digital surveillance practice around the globe.[1] I have long taken the position that a moratorium would enable a global regime of control and constraint to be developed, one that is consistent with international human rights standards.

Despite the overwhelming evidence of spyware's abuse, facilitated by an industry that operates in shadows of official secrecy and non-disclosure agreements, arguments continue to surface suggesting that robust constraints on spyware would somehow undermine counter-terrorism efforts, national security, and criminal law enforcement.[2] These are unsurprising, long-stated talking points of the commercial spyware industry, which has a strong interest in a status quo according to which global restrictions are practically non-existent. The arguments are self-interested, of course, but at least two should be refuted or contextualized if only to ensure a balanced consideration of the issues posed by commercial spyware.

---

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Surveillance and human rights), A/HRC/41/35, May 28, 2019, available at https://www.undocs.org/A/HRC/41/35.
[2] Some of these arguments are put forward by NSO Group, whose Pegasus spyware has been used repeatedly to interfere with human rights worldwide and which has been added to the Entity List by the U.S. Department of Commerce, as noted in the resolution's report. I am referring, for instance, to an April 13, 2023, letter from NSO Group to the Chair of the ABA's International Law Section.

First, the legal framework for human rights protection requires not only a legitimate interest in any given interference with privacy or expression; it also requires demonstrating legality, necessity and proportionality. National security, as an argument, is not a magic mantra that can be invoked to insulate surveillance practices from legal control. Under well-established requirements of international human rights law, including the so-called "three-part test" of the International Covenant on Civil and Political Rights (ICCPR), an interference with privacy or freedom of expression must be provided by law with specificity and accompanied by strict safeguards in place which sufficiently eliminate the risk of arbitrary interference (legality); be imposed to protect only legitimate aims, such as national security (legitimacy); and be proportionate to the aim pursued and the least intrusive instrument among those which might achieve the legitimate objective (necessity and proportionality).[3]

Even if one were to grant the industry its view of how its spyware protects national security – that it is "essential" to countering terrorism and other criminality – such an assertion only goes one third of the way toward making an argument for consistency under human rights law. (Of course, the rampant use of Pegasus spyware against journalists and human rights defenders, among others, deeply undercuts the legitimacy prong of the argument). It fails to address how such a powerful invasion of privacy and freedom of expression can exist in the absence of a legal framework authorizing or constraining its use. It fails to address why other, less intrusive law enforcement tools – including powerful surveillance practices that do not rely upon penetration and exploitation of one's private device – cannot achieve similar purposes without such risks of interference. Given the extraordinary invasions that spyware enables, providing not only historical but real-time access to all of one's personal device, mere assertions of state interest without more are entirely inadequate as a matter of human rights law. In short, any industry argument resting merely on *interest* or *national security* fails to grapple with the reality of how human rights law works and what it is designed to protect. The argument implies that national security interests operate to suspend the application of longstanding human rights law processes; the proposed resolution takes a strong stand against such an intolerable outcome.

Second, voluntary measures cannot on their own meet the requirements of international human rights law. Some companies in the spyware industry claim that their voluntary human rights compliance programs are consistent with the UN Guiding Principles on Business and Human Rights (UNGP)[4] and somehow justify their practices. However, spyware "human rights" policies, such as that promoted by NSO Group, fail to include at least the following minimum and essential programs required by the UNGP, leaving the risks of abuse of their products unaddressed. Perhaps most importantly, the UNGP provides that companies should "avoid infringing on the human rights of others" (Principle 11) and "[s]eek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships" (Principle 13). In the context of spyware, vendors should ensure that their customers are

---

[3] Human Rights Committee, *General Comment No. 34: Article19: Freedom of opinion and expression*, CCPR/C/GC/34, September 12, 2011, paras. 21-36, available at https://www.undocs.org/CCPR/C/GC/34; Human Rights Committee, *General Comment No. 16 (1988): Article 17 (Right to Privacy)*, CCPR/C/GC/16, April 8, 1988, paras. 3, 4, 7, and 8, available at https://www.refworld.org/docid/453883f922.html; and Human Rights Committee, *Views adopted by the Committee under article 5 (4) of the Optional Protocol, concerning communication No. 3163/2018*, CCPR/C/131/D/3163/2018, September 16, 2021, para. 7.4, available at https://www.undocs.org/CCPR/C/131/D/3163/2018. *See also*, Report of the Office of the United Nations High Commissioner for Human Rights (The right to privacy in the digital age), A/HRC/27/37, June 30, 2014, paras. 28, 29, 37, and 38, available at https://www.undocs.org/A/HRC/27/37.

[4] Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie (Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework), A/HRC/17/31, March 21, 2011, available at https://www.undocs.org/A/HRC/17/31.

using their products only in a way that meets the stringent requirements under international human rights law such as described in the three-part test. A mountain of evidence shows how spyware is used by customers lacking any meaningful constraint based on the rule of law, and yet the industry continues to market, sell, and transfer its products.

To be consistent with the UNGP, it is not enough to publish a policy and to assert, for instance, that it requires states to comply with human rights, or that it guides the selection of customers, if one is not prepared to disclose in detail the customers engaged, the steps taken, the abuse detected, and so forth. None of that actually follows from the mere adoption of a policy. Indeed, the UNGP calls upon companies to communicate how they address human rights risks with sufficient detail "to evaluate the adequacy of an enterprise's response to the particular human rights impact involved" (Principle 21). Spyware vendors thus should require their customers to agree to such disclosure as required by the UNGP as a condition of using their products and should not sell their products unless their customers agree to this. In reality, however, spyware vendors keep failing to make sufficient disclosure, using confidentiality obligations imposed by customers as excuses. As a result, evaluation of the effectiveness of their programs has remained utterly impossible.

Although I do not intend to burden you with an exhaustive list of gaps between the requirements under the UNGP and spyware vendors' voluntary human rights compliance programs (to the extent they exist), I would like to reiterate that the poor quality of self-regulation – if it can even be called that – further increases the need for a moratorium until a strong international regulatory framework is in place.

NSO Group suggested in its April 13 letter that it has "been actively collaborating with international human rights stakeholders for the past few years to develop a regulatory framework to promote the responsible use of cyber intelligence technologies." This may be so, though it does not identify those stakeholders (nor am I aware of any international human rights organizations "collaborating" with the industry, let alone NSO Group). To be sure, it has engaged in exchanges of letters with human rights mechanisms, including myself.[5] But generally the spyware industry has failed to provide meaningful information about their operations in specific cases of abuse. Companies have failed to make meaningfully verifiable commitments to human rights compliance. And yet still, the examples of abuse continue to pile up, calling into question the good faith of any claims of concern for the core values of human rights law in democratic societies and for the well-being of human rights defenders worldwide.

---

[5] *See, e.g.,* Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, OL OTH 52/2019, October 18, 2019, available at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24905; NSO Group, Re: NSO Human rights and Whistleblower Policies, NSO Group, December 10, 2019, available at https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=35041; Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, OL OTH 2/2020, February 20, 2020, available at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25079; NSO Group, Re: NSO Human Rights and Whistleblower Policies Responses to February 20, 2020 Letter, June 1, 2020, available at https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=35326; Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Working Group on the issue of human rights and transnational corporations and other business enterprises; the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on the situation of human rights defenders, AL OTH 211/2021, August 4, 2021, available at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26564; and NSO Group, Re: Joint Communication from Special Procedures, September 20, 2021, available at https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=36555.

The future of the rule of law in the face of extraordinarily invasive and powerful tools of surveillance depends on placing human rights at the center of the action to constrain spyware, and – as the proposed resolution makes clear – a moratorium on such tools is a critical first step.

I deeply appreciate the ABA's commitment to advocate for rule of law and human rights compliance and would expect that this resolution, if passed, will inspire other bar associations and policymakers around the world to take similar actions. Thank you very much for your consideration.

Sincerely,

David Kaye
Member, American Bar Association

cc: Members of the ABA House of Delegates
Members of the ABA Sections on International Law and Civil Rights and Social Justice