UC Irvine School of Law
International Justice Clinic:

Meeting the threat of mercenary spyware

November 30, 2022

SUMMARY OF PROCEEDINGS

On November 9, 2022 the International Justice Clinic at the University of California, Irvine, School of Law (UCI Law), together with Access Now, hosted a meeting of advocates and researchers working to curtail the human rights threats posed by the private spyware industry. Under the Chatham House Rule, around 40 participants from around the world who are experts in law, human rights research/advocacy, and security discussed their ongoing institutional and individual efforts to restrain state-sponsored digital surveillance by spyware and its infringement on the rights to privacy, freedom of expression, association, and other guarantees in international law.

Convened as a follow-up to the clinic's spring 2022 "Ending the Private Surveillance Threat" workshop series, participants discussed, among other topics, proposals for a moratorium or bans on the technology, domestic, regional, and international litigation, accountability for spyware vendors, and best practices for third party technology companies.

I. Moratorium and/or Ban of Spyware

Participants began the day discussing whether calls for a moratorium or ban are the right course of action.

It was widely believed that intrusive surveillance tools like Pegasus likely could never meet relevant standards because privacy intrusions must meet the tests of legality, necessity, and proportionality. In particular, a tool that indiscriminately accesses, or has the capability to

access, all information on a device could likely never be proportionate to meet international human rights requirements.

Given this assessment, participants discussed whether a ban would be appropriate to prevent the risk of a regulatory approach that would implicitly recognize legitimate uses of such spyware. A moratorium pending further policy developments, it was suggested, could be a more achievable interim goal. At the same time, some raised the concern that spyware bans could paradoxically force the industry underground and even further from compliance with international human rights. Some pointed out that the focus of the policy discussion could be the conditions of spyware use, oversight, and accountability, given the risks of delineating the per-se illegal spyware.

Any effort to regulate the private spyware industry at global scale would have to address, at a minimum, the following issues:

A. *Defining the Technology.* Participants reiterated the importance of a clear definition of spyware that would be subject to a ban or moratorium. In this connection, they discussed the challenges in defining the technology as limited to spyware that, like Pegasus, indiscriminately accesses all information on personal devices. Many agreed that technical experts need to be involved in defining the scope of spyware to prevent any potential negative implication. The Wassenaar Arrangement[1] and proposed Media Freedom Act in the EU[2] have articulated definitions of spyware might provide a useful definition to reference for policy measures although further examination of the scope of the technologies which fall under them would be needed.

[1] The Wassenaar Arrangement defines spyware as “intrusion software” that is “specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network- capable device, and performing” the extraction of data or information, from a computer or network- capable device, or the modification of system or user data” or “the modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.” The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, *List of Dual-Use Goods and Technologies and Munitions List*, 224, Volume II (Dec. 2021).
[2] Spyware under the European Media Freedom Act “means any product with digital elements specially designed to exploit vulnerabilities in other products with digital elements that enables the covert surveillance of natural or legal persons by monitoring, extracting, collecting or analysing data from such products or from the natural or legal persons using such products, in particular by secretly recording calls or otherwise using the microphone of an end-user device, filming natural persons, machines or their surroundings, copying messages, photographing, tracking browsing activity, tracking geolocation, collecting other sensor data or tracking activities across multiple end-user devices, without the natural or legal person concerned being made aware in a specific manner and having given their express specific consent in that regard.” Regulation of the European Parliament and of the Council, Chapter 1, Article 2, COM (2022) 457 final (Sept. 19, 2022).

B. *Unrestrained Surveillance.* Participants raised that the key concern with Pegasus-type spyware is that the technology cannot limit its data collection on the device. U.S. laws on police surveillance such as wiretapping require some minimization of data collected; however, such efforts demonstrably often fail due to a state's motivation for maximization of data collection. Furthermore, given that the scope of information accessed is so much more expansive than conventional surveillance such as wiretapping, minimization of data collection for the spyware is uniquely challenging. It was also raised that the perceived risk of indiscriminately accessing the information causes a chilling effect on potential targets' behaviors.

C. *Limitation of Export Controls as Regulatory Measure.* Participants noted that export controls can and should be more stringent, for example through reiterating both human rights harms and national security risks caused by the export of spyware. The Wassenaar Arrangement may be an appropriate locus for these kinds of discussions at the global level. Participants also pointed out some challenges and limitations in the effectiveness of export control regimes. For example, because Israel, where NSO Group is headquartered, is not a member of the Wassenaar Arrangement, the Israeli government's commitment to encourage restraint the export is, at best, unclear. Further, even if the Wassenaar Arrangement appropriately agreed to the scope of controlled items and framework for control, due to the non-binding nature of the agreement, states can decide whether and how strictly implement the agreement.

D. *Europe as Potential Leader in Moratorium.* The Rapporteur of the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee) has expressed in draft findings of the Committee that a moratorium on the use, sale, transfer, and acquisition of the technology should be adopted by the EU pending thorough investigation into past and current state-sponsored spyware use. The report also reiterates that strict regulation should be adopted to prevent the worst abuses. Participants expressed concerns about the potential implications of discretion of each member state, which the Rapporteur's draft report appears to allow. Participants will be following further developments and urging similar efforts in other policy domains.

E. *Israel's Role.* Participants discussed the vital role Israel plays in regulating and controlling NSO Group and other spyware developers within its jurisdiction. They raised the fact that because NSO Group requires permission from the national government to export its technology to approved countries, that it effectively operates with cooperation with the Israeli government.

II. Litigation

Participants discussed domestic, regional, and international litigation strategies, successes, and hurdles, and how such efforts may advance the goal of restraining the state's use of spyware.

A. *Sovereign Immunity Blocking Cases against Transnational Repression.* The legal doctrine of foreign sovereign immunity has hindered lawsuits brought against governments in foreign courts, including in the context of alleged uses of spyware against human rights defenders and others.[3] Legal developments in the UK,[4] as well as participant research projects, may suggest approaches to overcoming the barrier of sovereign immunity claims and allow for spyware cases to be pursued against foreign governments in domestic courts.

B. *Factual and Evidentiary Issues.* Participants discussed technical requirements to confirm and attribute spyware infections, noting the importance of preserving evidence on a victim's device after suspected infections. Participants noted that, in addition to forensic evidence, circumstantial evidence may also be particularly valuable, such as evidence of a licensing arrangement between a spyware vendor and a government, and demonstrable patterns of the state's oppression of journalists and human rights defenders. It was also suggested that the burden of proof should be shifted to the state in order to address legal attribution of infection to the state.

C. *Intangibility of Harms.* Participants noted that the chilling effect and psychological harms are particularly important to demonstrate to the court. Participants suggested news articles or reports which depict how spyware infection changed victims professional and personal lives would be useful for such demonstrations. Further sharing of evidence on such harms should be encouraged among researchers and advocates.

D. *Speed of Litigation.* Governments and spyware vendors have successfully dragged out cases with procedural and preliminary delays causing cases on behalf of victims to continue for years without arriving at stages of factual inquiry.

E. *Secondary and Tertiary Victims.* Participants highlighted additional victims harmed by spyware beyond the owner of an infected device, including all their contacts who are

[3] See, e.g., *Doe v. Fed. Democratic Republic of Ethiopia*, 851 F.3d 7 (D.C. Cir. 2017).
[4] *Al-Masarir v. Kingdom of Saudi Arabia* [2022] EWHC 2199 (QB).

also subject to potential surveillance by communicating with someone through a compromised device. Additionally, participants raised the broader harms implicated by the chilling effect of spyware on anyone who believes they could be targeted for surveillance. Participants raised the possibility of such victims being parties to future litigation.

F. *Litigation Targeting Purchasing Governments.* Participants highlighted and discussed the work of various organizations to pursue lawsuits or freedom of information requests for government disclosures of information regarding consideration, purchase, and use of NSO products. Such efforts have already resulted in some transparency in jurisdictions such as the United States and Mexico.

G. *Norm Development at the United Nations Level.* Participants pointed out that some gaps are seen in the norms at the United Nations level and those in other jurisdictions such as the European Court of Human Rights, especially in the context of digital surveillance. Participants suggested that United Nations mechanisms, such as individual complaints and shadow reporting to treaty bodies, could be used to contribute to the norm development, as IJC is seeking to do.

H. Limitations of Redress from Domestic Courts. Many victims express a desire to see the spyware threat ended, certain abusive countries banned from acquiring surveillance tools, formal acknowledgements and even apologies for the clandestine surveillance they suffered. Not all domestic courts address such remedies, that is, beyond compensation. It was noted that, to address the injustice of spyware, a multi-faceted approach by which individual litigation forms but one part would be required.

I. Litigation and Future Deterrence. Participants discussed the limitations of litigation beyond individual victim advocacy. There is an open question of whether individual litigation can deter future threats or pressure bad actors to cease spyware attacks. Nonetheless, participants confirmed that litigation could lead to actions which directly deter misconduct such as effective legislation or sanction against spyware vendors.

III. Accountability for Spyware Producers and Investors

Participants discussed various avenues to hold spyware vendors and investors accountable.

A. *Private Vulnerability Mining and Trading Needs Regulation.* Vulnerability mining and trading is a part of the development process of spyware, which exploits identified vulnerabilities of hardware or software. Businesses' self-regulations in this area must be accompanied by rigorous state regulation, if not bans of use.

B. *Limitations of UNGPs.* Many participants shared the view that the United Nations Guiding Principles on Business and Human rights is necessary but insufficient.

C. *Expansion of Spyware Vendors Disclosure.* Environmental, Social, and Corporate Governance initiatives could include requirements for companies to disclose their connections with rights abusers. Such efforts could inform the public of ethical problems with their potential investments as participants discussed upcoming opportunities to include spyware concerns in ESG efforts.

D. *Investor accountability.* Participants discussed ideas of identifying investors in spyware companies as an important avenue for constraining the spyware industry. Participants acknowledged some hurdles to litigating or requesting sanctions against investors, and reiterated the importance of researching the financial flow and naming and shaming investors who fund spyware vendors.

IV. Best Practices by Third Party Technology Companies

Participants discussed the role of third-party technology companies in combating spyware. As infections are often launched by exploiting vulnerabilities in devices and digital products like WhatsApp and Apple iPhones, third party technology producers have a vested interest in protecting their customers from spyware infections through exploitations of their products.

A. *Best Situated to Address the Problem.* Because companies have unique technical insights and access, economic resources, and leverage with policymakers, they may take a greater role in combating the threat. Participants discussed the need to encourage such leadership. The separate litigation brought by Meta and Apple against NSO Group provide an example of company engagement and protection of user rights and equities.

B. *Collaborations with Civil Society.* Participants first expressed gratitude for various collaboration with civil society and technology companies such as Apple's $10 million

grant to assist civil society,[5] Google's Project Zero,[6] and work to ensure notification to spyware victims.[7]

C. *Notifying Victims.* Many companies hesitate to disclose suspected infections with victims and the public given the sensitivity of the issue for their security. Such disclosures are essential to victim protection and advocacy. Participants discussed ongoing inquiries into how to encourage such practices.

D. *Notifying Unpatched Vulnerabilities to Regulatory Bodies.* Participants discussed tech companies' responsibilities to notify identified and unpatched vulnerabilities in their products to competent regulatory bodies so that governments can know who has which vulnerabilities and prevent and sanction the abuse of vulnerabilities.

E. *Potential Benefit of Group Engagement with Tech Companies.* Participants stated the need for greater transparency and coordination between companies of their practices upon discovering that vulnerabilities in their products have been exploited to surveil customers. However, they acknowledged business concerns of appearing to encroach on anti-trust laws and thus concluded that civil society should step up further in this domain to inform and instruct companies of best practices for preventing and addressing the issue.

V. Conclusion

Participants confirmed that their continuous efforts in the immediate and longer term are indispensable to address the global problem posed by the private spyware industry, and look forward to the upcoming collaboration with the full range of civil society organizations.

[5] *Apple expands industry-leading commitment to protect users from highly targeted mercenary spyware*, Apple (Jul. 6, 2022)
[6] Ian Beer & Samuel Groß, *A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution*, Project Zero Blog (Dec. 15, 2021).
[7] *WhatsApp sues Israeli firm, accusing it of hacking activists' phones*, the Guardian (Oct. 9, 2019) ("The organisation has begun approaching members of civil society who were affected by the alleged hacks.")