UCI Law

UNIVERSITY OF CALIFORNIA, IRVINE SCHOOL OF LAW

ENDING THE PRIVATE SURVEILLANCE THREAT

UC IRVINE SCHOOL OF LAW WORKSHOP SERIES

SUMMARY OF PROCEEDINGS

On March 9, 16, and 21, 2022, the International Justice Clinic at the University of California, Irvine, School of Law (UCI Law) hosted three workshops on the global threat the private surveillance industry poses to human rights. The workshops, conducted under the Chatham House Rule, brought together experts from law, human rights research/advocacy, and security. The participants shared their views and expertise regarding the sale and use of spyware, benefits and challenges of addressing human rights violations in domestic justice systems, and the role of private sector actors, including investors, in connection with the surveillance industry. This workshop series, developed with the support of UN Special Rapporteur on the right to freedom of expression Irene Khan, concluded with a discussion of a shared agenda to constrain the spyware industry worldwide.

WORKSHOP 1: INTERNATIONAL LEGAL FRAMEWORK AND REGULATION

Participants began the workshop series by discussing whether spyware technologies could ever meet the requirements of international human rights law. Some took the view that spyware technologies with unimpeded reach into personal devices (such as but not limited to the NSO Group's Pegasus malware) fundamentally fail human rights standards and deserve to be banned. Others felt 'the cat is out of the bag' and that an extensive regulatory regime would be an appropriate target for advocacy. Still others concluded that a targeted, highly constraining regulatory regime could in effect constitute a ban of technologies with certain, irredeemably violative features. The discussion addressed the following ideas and arguments:

I. *Pegasus-grade Spyware Fails Human Rights Standards.* The private surveillance industry and its intrusions on individual privacy must be evaluated under the three-prong legality, legitimacy, and necessity test drawn from international human rights law, especially Article 19 of the International Covenant on Civil and Political Rights (ICCPR), and the necessity and proportionality test of the ICCPR's Article 17. Private surveillance products like the NSO Group's Pegasus, it was argued, can never meet these requirements.

Legality. Any restriction on a right to privacy and freedom of expression must be provided by law in a manner that is precise, public, and transparent. Overly broad laws that do not provide citizens with a warning about what conduct may be

regulated fail to meet this prong. Additionally, no law can be consistent with international human rights if it grants a State indiscriminate and uncheckable surveillance power.

Legitimacy. States must demonstrate that a fundamental right is limited only in the pursuit of a legitimate interest. While the NSO Group claims that Pegasus is used for national security interests and law enforcement, the spyware is often used to surveil human rights advocates, journalists, and political dissidents. Invoking national security cannot be a blanket justification, a *carte blanche,* for interference with human rights.

Necessity and Proportionality. States must demonstrate that Pegasus is necessary to protect legitimate interests and is the least restrictive means of achieving that interest. Because Pegasus offers indiscriminate access to all of an individual's information, spyware like it can never meet this prong. There will always be a less restrictive measure than providing a state with unrestrained, possibly unconstrained, access to an individual's personal information.

II. *The Troubling Nexus Between States and Private Industry.* By developing and selling novel and intrusive surveillance technologies, private companies are equipping States with capabilities that should exclusively belong to States. While the exploitation of device vulnerabilities is often illegal in domestic contexts, States tacitly approve of the private surveillance industry because they benefit from it. By allowing private companies to develop and improve capabilities that should solely belong to States, governments are able to avoid rigorous transparency and accountability norms. At the same time, private corporations seek to avoid liability by invoking State oversight even where non-existent.

III. *The EU Regulatory Framework.* EU law governs the sale of controlled products when they are to be exported to countries outside of the Union. However, this framework was not designed for cyber-surveillance or the human rights implications they pose; the EU only recently amended its regulatory framework to include a new category that is meant to encompass cyber-surveillance items. The European Commission requires that member-countries seek authorization for the dual-use technologies discussed in current legislation as well as for technologies not currently listed in legislation annexes "if the exporter has been informed by the competent authority that the items in question are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of human rights and international humanitarian law." The Commission also requires an annual report detailing which member states permitted exports, the number of applications received for each type of surveillance technology, and the destination of the export. This process was said to promote transparency and consistency among state standards and requires companies to exercise human rights assessment due diligence (though these standards can be vague).

IV. *Importance of Domestic Regulations.* Domestic regulations serve an essential function in regulating and strengthening export controls. Regulation of the private surveillance industry can be treated similarly to the regulation of weapons or nuclear missiles. However, relying on domestic regulations poses challenges given the dramatic variations in state structures, and interest in preventing state usage of spyware by legislative or policy means. Some states maintain an interest in the private surveillance industry that must be taken into consideration because, as in the case of Israel, the state permits private surveillance companies to stay in business and can use such companies as strategic foreign policy tools. Effective domestic regulatory systems must consider how private surveillance tools may be used and abused in a client country purchasing the spyware, a process that should include a thorough evaluation of the country's human rights record.

WORKSHOP 2: DOMESTIC REMEDIES

Participants, many of whom enjoyed experience in surveillance-related litigation and policies, shared their perspectives on the benefits and limitations of litigation to address the global spyware threat. The discussion addressed the following:

I. *Litigation Avenues.* Individuals and companies around the world have pursued legal remedy in domestic courts for alleged illegal surveillance by state actors facilitated by private surveillance tools. These lawsuits target two different categories of defendants: state actors who have allegedly used spyware for surveillance, and spyware companies for their role in state-sponsored surveillance. To date, petitions against these defendants have been filed in family, civil, and criminal courts alleging illegal surveillance of individual's devices.

The workshop discussed several instances of litigation: French prosecutors opened an investigation following the 2021 reports of French devices potentially targeted by Pegasus, including the phone of President Emmanuel Macron. The Indian Supreme Court ordered an investigation into state sponsored surveillance following the reports of Pegasus infections and individual suits from alleged spyware victims and may demand that the government admits the purchase of the technology. In the United States, spyware companies have faced civil litigation for their role in state-sponsored attacks. Israel's weapons export policies have been legally challenged by Amnesty International and others for granting export licenses to NSO Group.

II. *Litigation Hurdles.* Several legal hurdles in domestic courts must be addressed in litigation involving surveillance companies and state actors. An inherent risk of litigation is the uncertainty with which precedent may be established given the variety of ways that litigation can unfold, especially with the number of market players who have competing interests. In addition to the inherent risk of litigation, specific doctrines make it difficult for claimants to obtain remedies against states or private surveillance companies.

Sovereign Immunity Shields State Actors. Participants identified sovereign immunity as a significant hurdle to legal remedy for victims of state surveillance.

Sovereign immunity may protect state actors from the jurisdiction of foreign courts. This has occurred in the United States, and blocked relief for victims even with US citizens as victims of foreign government hacking while they were on US soil. Experts discussed the possibility of legislative action to develop a new spyware/surveillance exception to foreign sovereign immunity, much as some states have adopted statutory exceptions in the context of terrorism and other serious violations of international law.

Attempts to Extend Sovereign Immunity Protections. Private surveillance companies have claimed that this immunity extends to them when their product is used by a state actor. While claims continue along these lines, such a derivative immunity claim has been rejected by the U.S. Ninth Circuit Court of Appeals in *WhatsApp Inc. v. NSO Group,* 17 F.4th 930 (9th Cir. 2021). In this case, NSO Group has attempted to avail itself of foreign sovereign immunity and argue that it is an arm of the Israeli government. NSO Group has sought certiorari in the U.S. Supreme Court.

Drawbacks of Reliance on Big Tech. Litigation against private spyware companies may offer some promise for victims. However, participants cautioned against relying on tech giants like WhatsApp and Apple, which have pursued their own suits against surveillance companies for exploiting vulnerabilities in their products to illegally surveil their customers. Though litigation from Big Tech companies helps tackle the problem with significant resources and draws mainstream attention to the problem, it empowers these companies to shape law and policy in this domain to business interests, and not necessarily the interests of human rights.

Difficulties with Identifying Injury. The nature of private surveillance makes it difficult to identify the injury typically necessary for a plaintiff to have standing in court. While there are instances where the use of private surveillance technology has resulted in tangible injury, such as imprisonment, in most cases such surveillance may go unnoticed. Participants discussed the challenge of attributing a malware attack and identifying a specific defendant. The inability to identify a cognizable injury for the purpose of standing creates major barriers to recovery. The secrecy surrounding private surveillance technology due to its relationship with State actors hinders litigation by impeding processes like discovery. This, combined with perpetrators' deep pockets, can result in many cases being dismissed or settled.

Expertise Shortage. Participants noted a shortage of technical experts who understand and can testify in court about specific malware attacks. Remotely-deployed spyware is by its clandestine nature difficult to trace and to prove. Plaintiffs need more experts in the area to aid with proving their claims.

III. *The Potential Paradox of Litigation.* Some noted that it is important to consider whether litigation risks creating dangerous precedents in this area that could effectively act as a "rubber stamp mechanism" that offers a legal path for governments hacking that evades legal accountability. For example, participants discussed cases in the UK that addressed a spyware issue but recognized that some forms of government hacking could be licit under national law, an unfortunate outcome. Alternatively, participants raised concerns that any litigation may not prove effective in stopping state-sponsored surveillance or helping victims.

IV. *Legislative Action.* Experts discussed the possibility of legislative action to introduce an exception to foreign sovereign immunity in the context of transnational harm to allow victims to pursue remedy against state actors in domestic courts. Some entertained imposing obligations on technology companies to disclose state-sponsored malware attacks using their platforms. Participants discussed the need for a legislative carve out for sovereign immunity for transnational harms. In November 2021, the UK introduced a new cyber security bill to enhance device security. The legislation would regulate the manufacture and sale of devices which may be vulnerable to cyber security attacks. The regulator will have the authority to mandate further security requirements in light of new threats.

WORKSHOP 3: PRIVATE ACTORS

Participants discussed the duties or responsibilities of companies whose products or services are exploited or corrupted to facilitate digital surveillance. Participants agreed that corporations should collaborate with one another to develop a set of best practices and provide recommendations on how to handle spyware infections. Key points of the discussion addressed the following:

I. *Investor Accountability.* The Israeli-based NSO Group is partially owned by investors, as other spyware companies may be. Participants highlighted the power of divestment campaigns, recalling recent divestment discussions amongst investors with stakes in the spyware industry. Investors could significantly rein in the private surveillance industry by divesting from or refusing to fund surveillance companies, thus impacting funding sources for producers of these dangerous and uncontrollable surveillance tools. Responsible investor action can be spurred by public pressure. One way of tackling this problem can be through collective demand for divestment from funds that directly invest into private spyware technology or have ties to these first through other financial arrangements.

II. *Technology Companies Initiate Litigation*. Technology companies whose products are utilized by spyware developers to target individuals for surveillance are well positioned to pursue legal action. Spyware often accesses devices through vulnerabilities in popularly used devices and platforms. To date, multiple companies have sued spyware producers for misusing their products to illegally gain access to devices without the device owner's knowledge. Companies, as opposed to individual victims, are well positioned to litigate. Individual victims face a significant resource asymmetry when challenging surveillance

malware companies and state actors. Technology companies, on the other hand, tend to have more resources and technological expertise that can aid successful litigation.

Companies Take Action. Companies have worked with civil society organizations (CSOs) to identify and notify victims targeted by Pegasus. Companies have also notified the broader public by filing lawsuits and publicly calling for changes in oversight within the public surveillance industry.

Drawbacks to Litigation by Companies. Companies are equipped to litigate claims against private surveillance companies like NSO because of their abundance of resources. However, the objectives of companies and individuals are not always aligned. For example, seeking permanent injunction does not reach the fundamental issue of the use of vulnerabilities for an offensive purpose (*Apple v. NSO*) and instead, companies should target this offensive use without risking the legalization of any use of vulnerabilities. Litigation presents certain risks that need to be kept in mind: (1) there is always a risk of a negative outcome, (2) the outcome can legitimize bad behavior, (3) companies that seek injunctions may win lawsuits, but the underlying problem of unlawful surveillance will not be addressed.

III. *Organizing Technology Industry Responses.* Participants discussed creating a standardized set of best practices for technology companies whose users are surveilled through their products. Such standardized responses could create mechanisms for sharing information regarding attacks with the community and policymakers and advocating greater industry oversight in concert with CSOs as recommendations to help end the private surveillance threat.

IV. *Effectively Notifying Victims*. Participants agreed that companies should adopt effective notification protocols and inform victims of privacy violations and data breaches. Participants noted that notifications that merely communicate the fact or possibility of infection are insufficient. An effective notification should include additional information about action steps necessary to improve the security of a device as well as information regarding litigation or other redress options. However, while mass notifications contribute to transparency and allow ordinary citizens to become aware of surveillance attacks, notifications can also lead to public panic and could implicate the company undertaking notification with interference with "legitimate surveillance." Several participants believed this could be an effective area to develop joint work around in order to create stronger notification norms.

V. *International Code of Conduct as a Framework*. Participants discussed the International Code of Conduct (ICoC) for Private Security Companies and other Security Service Providers (PSCs). The code is an initiative launched by the International Code of Conduct Association, which was launched by the Swiss Government to address the private military contractor industry. The Code of Conduct sets standards for PSC behavior and recognizes the potentially positive and negative consequences private security companies have for their clients and local populations. Some noted that the Code of

Conduct as applied to private mercenaries was distinct in one key way – that private mercenaries have a physical presence with the ability for independent verification, whereas private surveillance operates with limited detection. Participants expressed doubt about this framework as it applies to private surveillance because private surveillance can operate completely undetected without any perceivable injury.

WORKSHOP 4: CONCLUSIONS

Participants concluded the workshop series with an open-ended discussion about next steps in the context of research and advocacy. There was a consensus on the value of sharing information and collaboration, and the International Justice Clinic plans to create an online hub to enable the sharing and updating of information within the community of advocates for addressing the spyware industry. The concluding discussion centered around the following questions:

I. *What may advocacy for a ban or moratorium of private spyware look like?*

In order to push governments to adopt strong export controls to ban private surveillance, advocates should bring attention to how private surveillance actually undermines national security. Advocates may continue to raise public awareness of the incompatibility of the private surveillance industry with human rights norms to lobby and advocate for State action. A good example of State action to regulate private surveillance is the US Department of Commerce's Bureau of Industry and Security action to ban trade with NSO Group.

II. *What may effective regulation look like?*

Effective regulation will require a human rights assessment of all product development and sales. States could adopt legislation imposing licensing and disclosure requirements as well as judicial oversight over spyware technology use. Judicial oversight may include asking spyware companies to disclose information about their sales, targets, clients, and information collected by their products. Legislators especially should balance spyware victims' privacy concerns with the need for transparency about infections.

III. *How can divestment from private equity groups financing industry be encouraged?*

Advocates may initiate divestment campaigns by investigating what investment funds and private equity firms buy or invest in private surveillance. Advocates can encourage divestment by highlighting the inherent risks of investing in a volatile industry that may be subject to litigation, stringent regulations, or even a ban.

IV. *What may effective litigation efforts include?*

Advocates can directly support litigation against private spyware companies by sharing knowledge, expertise, and providing technical assurance and expert testimony. Lawyers and advocates should highlight the discovery challenges associated with spyware cases and urge

(1) technology companies to disclose what happens during an attack and (2) private surveillance companies to disclose what information is provided to state clients. Additionally, advocates could propose legislation that would prohibit exploitation of security vulnerabilities to counteract any possible adverse precedent.

V. How to avoid sovereign immunity concerns?

Advocates may highlight the dangers of extending sovereign immunity protections to private actors, even if their services are used by States. Also, advocates could propose amendments to the sovereign immunity doctrine that would allow suits against States that fail to regulate the sale and use of private surveillance tools.

VI. What may an effective corporate response to an infection look like?

Companies could create a set of best practices regarding identifying, mitigating, and preventing spyware attacks. Companies could commit to notifying all affected victims, publicly acknowledge security breaches, conduct internal investigations, and share results with the community and policy makers. Companies may also continue strengthening their security and promote greater transparency and work in concert with civil society to advocate against private surveillance.

	Issue	Steps/Areas of Collaboration
1	What may advocacy for a ban or moratorium of private spyware look like?	- Raise awareness of incompatibility of private surveillance industry with human rights norms - Bring attention to how private surveillance actually undermines national security to push governments to adopt stronger export controls to ban private surveillance - Lobby and advocate for State action (e.g. the US department of Commerce action re the NSO group)
2	What may effective regulation look like?	- Require human rights assessment of all sales - Adopt legislation imposing licensing requirements and disclosures - Adopt legislation that requires judicial oversight over spyware technology use - Impose reporting requirements on companies - Consider privacy concerns while demanding transparency about infections
3	How can divestment from private equity groups financing the industry be encouraged?	- Raise awareness of what investment funds and private equity firms buy or invest in private surveillance - Advocate for divestment - Highlight inherent risks of investing in a volatile industry that may be subject to stringent regulation and litigation at any moment
4	What may effective litigation efforts include?	- Share knowledge and expertise by providing technical assurance and expert testimony - Advocate for transparency in private actor obligations to establish personal jurisdiction - Advocate for stringent data obligations on private companies on both sides: targeted companies should disclose what happens during an attack and private surveillance companies should disclose what information is provided to state clients - Propose legislation to ban the exploitation of vulnerabilities
5	How to avoid sovereign immunity concerns?	- Limit private corporations ability to claim protection of sovereign immunity where they are regulated or utilized by States - Limit foreign sovereign immunity for states that fail to effectively regulate the use of private surveillance technology or place export controls on its sale to foreign entities
6	What may an effective corporate response to an infection look like?	- Create a set of best practices to monitor for and protect against attacks - Notify affected victims - Publicly call out the breach - Share results with the community and policy makers - Work towards stronger security - Promote greater transparency and oversight for private company practices to strengthen security - Work in concert with CSO partners to advocate against private surveillance