Clipping Pegasus's Wings

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

Introduction

Surveillance technologies available on the international market include spyware, biometric identification, computer interference, network surveillance, and many others. Among others, spyware is alarmingly powerful and increasingly available. Examples of their power have captivated public concern globally with the extensive reporting and research from Citizen Lab, Amnesty International, and Forbidden Stories' Pegasus Project.[1] Surveillance technology has garnered concern among human rights experts for years.[2] Nonetheless, the proliferation of surveillance tools and vendors has expanded the availability of these invasive technologies to a wide range of states, including those with worrisome human rights records.

The type of spyware like the Israeli NSO Group's Pegasus is arguably the most powerful and sophisticated spyware. It covertly infects an individual's device and enable unlimited access to data stored on or connected with the device, often without leaving traces. Pegasus and similar kinds of tools raise questions of compatibility with international human rights law, particularly those norms that guarantee rights to privacy, freedom of opinion and expression, and freedom of assembly, among others.

UCI Law's International Justice Clinic has been tackling this issue through its research, education, and public advocacy. Since Professor Kaye's 2019 Report to the United Nations, the Clinic has explored how the technology implicates international human rights law. Professor Kaye, with the Clinic's support, has provided expert testimony and analysis to courts and bodies around the world, including the Indian Supreme Court, U.S. Court of Appeals for the D.C. Circuit, and most recently before the European Parliament's PEGA Committee.

This website and its accompanying series of reports seeks to contribute to ongoing efforts to address and constrain the global threat the private spyware industry poses to international human rights. Our work focuses on products like Pegasus though the spyware threat is goes well beyond one single company or malware. We aim to highlight a range of work on the digital surveillance

[1] Forbidden Stories, About the Pegasus Project, https://forbiddenstories.org/about-the-pegasus-project/.

[2] See, e.g., Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40 (Apr. 17, 2013)¶ 3, and Surveillance and human rights, A/HRC/41/35 (May 28, 2019) ¶ 6.

issue, summarize some relevant developments, and provide support to other researchers, advocates, and concerned members of the public.

Our reports consist of five sections. The first section describes the particularly concerning features of intrusive spyware. Second, we propose a legal framework which concludes that the intrusiveness and indiscriminate nature of spyware like Pegasus runs counter to the standards of international human rights law, counseling its ban. We then assess litigation and policy effort at the national, regional, and international level that have been launched to address the problem in the third section. The fourth section discuss how private companies are required to respond to the crisis given their human rights obligations. Finally we provide a roadmap of various short-term and long-term measures to constrain the spyware threat in the fifth section.

Groundbreaking forensic work by Citizen Lab and Amnesty Tech, advocacy by civil society, and the UN expert engagement are leading to visible regulatory actions against spyware. For example, in May 2023, the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee) has, after the year-long investigation, adopted the final report and a set of recommendations, including regulatory framework applicable to the use, manufacture, and sale of spyware.[3] In the United States, the Biden administration has issued in March 2023 several restrictive measures domestically and has articulated a desire to further take concerted action with other countries.[4] In April 2023, Costa Rica has joined the call for a moratorium.[5] In the coming year, we expect many major developments in restraining the spyware industry and its customers.

This report was researched, drafted and coordinated a number of UCI Law students, led by Andrea Cervantes and including major work by Anna Setyaeva, Mason Schoeppl, Lilla Lavanakul, Srivats Shankar, Ethan Itzhaki, Gabriel Lazo, James Tsang, Spencer Levitt, helped bring the report to the final stages. Professors David Kaye, Sofia Jaramillo Otoya, and Hinako Sugiyama, supervised the project.

[3] Press Release, PEGA Committee, Spyware: MEPs sound alarm on threat to democracy and demand reforms (May 9, 2023), https://www.europarl.europa.eu/news/en/press-room/20230505IPR84901/spyware-meps-sound-alarm-on-threat-to-democracy-and-demand-reforms.

[4] Tim Starks, How the Biden administration wants to tackle foreign commercial spyware, Wash. Post (Nov 22, 2022), https://www.washingtonpost.com/politics/2022/11/22/how-biden-administration-wants-tackle-foreign-commercial-spyware/.

[5] Access Now, Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology (13 April 2022). https://www.accessnow.org/press-release/costa-rica-first-country-moratorium-spyware/.