House Foreign Affairs Committee
Tom Lantos Human Rights Commission

Hearing
on
"The State of Exception in El Salvador: Year Five"

April 16, 2026
2:00 PM
1334 Longworth House Office Building

Statement for the Record
Nadine Farid Johnson, Policy Director
Knight First Amendment Institute at Columbia University

Chairman McGovern, Chairman Smith, and Members of the Commission:

I am the Policy Director of the Knight First Amendment Institute at Columbia University, which works to defend the freedoms of speech and the press in the digital age. I respectfully submit this statement for the record in conjunction with the subject hearing to underscore the threat posed by the use of spyware to free expression and press freedom around the world, Including in El Salvador.

I know something about this because my colleagues represent journalists and others associated with *El Faro*, an independent news organization founded in El Salvador. Some of the most courageous journalists in the world write for *El Faro.* Per the International Press Institute, *El Faro* is a "paragon of investigative journalism" known for "fearless coverage of violence, corruption, inequality, and human rights violations." The outlet's coverage of such abuses in Central America has earned it the gratitude of readers all over the world—as well as the enmity of authoritarian governments, including its own. As detailed in the Inter-American Commission on Human Rights' Resolution 12/2021, which granted precautionary measures in favor of 34 members of *El Faro* deemed to be at "serious, urgent risk of suffering irreparable harm to their human rights," the Bukele regime engaged in an extensive campaign of "constant stigmatization, harassment, [and] criminalization" against *El Faro*'s journalists, also initiating a blackout against the outlet and engaging in the surveillance and monitoring of its members.

The Bukele regime's intimidation campaign against the journalists encompassed a particularly insidious and invasive form of surveillance: Between June 2020 and November 2021, at least 22 people associated with *El Faro* were the targets of extensive spyware attacks. Spyware is malicious surveillance software that can be installed on a target's mobile phone remotely and surreptitiously, without their action or knowledge, and then used to covertly track, trace, and access their devices. The iPhones of the *El Faro* members targeted by spyware were accessed remotely and surreptitiously. The members' personal and professional communications and

activities were monitored, and their personal data was stolen. These attacks often occurred when the journalists were engaging with confidential sources, including contacts at the U.S. Embassy in San Salvador, and the attacks intensified around the publication of major stories exposing corruption and other abuses by the Salvadoran government, including the Bukele regime's secret negotiations with gangs in the country.

The spyware used to target the *El Faro* journalists is called Pegasus. Pegasus is the signature product of NSO Group Technologies Limited, a company incorporated in Israel in 2010 which has recently come under U.S. leadership. NSO Group's own marketing materials have noted that Pegasus can be used to remotely and covertly surveil and extract contact details, text messages, instant messages, notes, emails, web-browsing activity, files, and passwords; monitor phone and VoIP calls and user activity on applications including WhatsApp and Facebook; track and log a device's GPS location; and activate the device's microphone and camera to record sound and photographs. Pegasus also facilitates access to cloud services—including those based in the United States, such as iCloud, Google Drive, and Facebook Messenger—allowing access to documents and photographs stored on those cloud servers unbeknownst to the phone's user.

Independent researchers verified that the *El Faro* members were targeted through "zero-click" attacks, using exploits that installed Pegasus remotely and without relying on the targeted user to download it by clicking a link. The nature of these attacks makes it practically impossible for people to protect themselves against them. In continually seeking to overcome security patches, spyware companies like NSO Group undermine cyber defenses and trust. Spyware companies do this work by exploiting and abusing the infrastructure of U.S. based technology companies; NSO Group, for example, has admitted that it employed a team to study Android devices and applications like Meta's WhatsApp to identify vulnerabilities that would allow it to use those applications to attack end users.

The harms facing those targeted by spyware are extensive. As the experience of the targeted El Faro employees demonstrates, spyware attacks upend and disrupt victims' lives and work. The journalists' safety, and the safety of their colleagues, sources, and families, were compromised. Their mental and physical health also suffered as a result of the attacks.

The impact reverberates further as well. *El Faro* enjoys a broad readership, not only in El Salvador, but also in Central America, the United States, and other regions around the globe. The outlet had to reconfigure its approach to news reporting as a result of the spyware attacks and the Bukele regime's campaign against it, working in the face of serious and ongoing threats to produce investigative journalism important to its global audience, hundreds of thousands of whom are in the U.S. alone.

Seeking redress for the harms they suffered as a result of the Pegasus attacks, 18 members of *El Faro* filed suit against NSO Group in late 2022. Represented by some of my colleagues at the Knight Institute, the *El Faro* plaintiffs alleged that NSO Group's development and deployment of the spyware violated, among other laws, the Computer Fraud and Abuse Act (CFAA), which

prohibits accessing computers without authorization, and argued that the case belongs in a U.S. court because NSO Group's development and deployment of Pegasus involved deliberate and sustained attacks on the U.S. infrastructure of U.S. technology companies in violation of U.S. law. To date, however, the case remains tied up in preliminary procedural disputes. As a result, the *El Faro* plaintiffs still lack clarity on what information was accessed and extracted from their devices and confirmation of the identity of the client with whom NSO Group carried out the spyware attacks.

The story of El Faro and El Salvador is an example, not an outlier. Governments may pledge they are using spyware for salutary aims, but in fact, many governments around the world use spyware to surveil journalists, human rights advocates, and political opponents, often in the service of broader campaigns of political intimidation and persecution. NSO Group's spyware has enabled these governments to conduct transnational repression, reaching across borders to stifle dissent. It has been used against journalists in Hungary, human rights activists in Kazakhstan, and Saudi political dissidents in Europe and North America. Groups including the University of Toronto's Citizen Lab, Amnesty International, and Access Now have documented many other instances in which authoritarian governments used NSO Group's spyware to quash dissent across sovereign borders. The egregious nature of its actions and the threat posed by Pegasus led the U.S. Department of Commerce to add NSO Group to its "Entity List," restricting NSO Group's ability to conduct business in the U.S. due to the risks such activities would pose to U.S. national security or foreign policy interests.

Nor is NSO Group alone. In recent years, the supply of spyware to authoritarian and other rights-abusing governments by mercenary spyware companies has become a grave and urgent threat to human rights and press freedom around the world. It is also a lucrative business: although estimates about the size of the industry vary, as of 2021, NSO Group had a valuation of approximately $2 billion. According to the Carnegie Endowment for International Peace, 74 governments procured spyware between 2011 and 2023 from a variety of companies, including FinFisher, Hacking Team, and Cellebrite, among others. NSO Group alone grants foreign governments the ability to spy on approximately 12,000 to 13,000 people annually. And the industry's reach is being amplified; as the industry's top players have faced increased scrutiny from governments and civil society, second-tier firms and hacking groups have turned to open-source code and low-cost tools to carry out spyware attacks. The uptick in easily deployed, malicious programs harms the digital ecosystem and increases the likelihood individuals will be victimized.

Like the *El Faro* plaintiffs, individual victims of other spyware attacks have faced procedural obstacles in U.S. federal court, even when the development and deployment of the spyware relied on the subversion of technological infrastructure inside the United States. Several early cases brought by victims have been dismissed in U.S. courts altogether, either because courts concluded that NSO Group was not subject to personal jurisdiction in the United States or that the case would be more convenient to litigate in Israel or elsewhere. These preliminary procedural challenges slow or even preclude the cases from reaching the merits, leaving victims

without redress for the harms to their privacy, security, and expressive freedom caused by the Pegasus attacks against them.

The hesitation exhibited by the courts in these cases highlights the opportunity for policymakers, who should address this fundamental imbalance and create a level playing field for spyware victims, allowing a pathway to redress.

Congress has acknowledged the concerns raised by the misuse of commercial spyware, but has yet to offer guidance to federal courts grappling with the procedural questions that the attacks on U.S. persons and others raise. The Computer Fraud and Abuse Act (CFAA) offers one vehicle for Congress to act in support of individual spyware victims and clarify a pathway for redress in U.S. courts, via the codification of a venue right for victims who were targeted via the exploitation of a software vulnerability in their devices.

Characterized as an "anti-hacking statute," the CFAA prohibits, *inter alia*, obtaining information through unauthorized computer access; engaging in computer-based frauds through unauthorized computer access; and knowingly causing damage to certain computers by transmission of a program, information, code, or command. While the law was enacted well prior to the development of readily deployable spyware, particularly the "zero-click" technology that powers Pegasus and some other commercial spyware, courts have held that the Act protects against the type of unauthorized access facilitated by these invasive technologies.

The exploitation of U.S. companies' technologies to enable the unauthorized surveillance and extraction of data from individuals' devices harms U.S. economic and security interests. At a minimum, it should create a threshold from which victims of spyware abuse can seek redress in U.S. federal courts. Congress should amend the Computer Fraud and Abuse Act to clarify that, in cases brought by spyware victims against spyware manufacturers that developed their spyware or deployed it against those victims through use of the software, services, or servers of U.S. companies, (i) venue is proper in the United States, and (ii) the spyware manufacturer should be deemed to have consented to the U.S. court's jurisdiction. By amending the CFAA in this limited way, legislators would signal their understanding of the challenges facing spyware victims, acknowledge the threat to U.S. economic, policy, and security interests posed by the unregulated use of this technology, and offer procedural guidance on this issue for federal courts.