EFF to Ninth Circuit: Don't Shield Foreign Spyware Company from Human Rights Accountability in U.S. Court

Sophia Cope and Andrew Crocker ⋮ 5-6 minutes ⋮ 8/2/2024

Legal intern Danya Hajjaji was the lead author of this post.

EFF filed an amicus brief in the U.S. Court of Appeals for the Ninth Circuit supporting a group of journalists in their lawsuit against Israeli spyware company NSO Group. In our amicus brief backing the plaintiffs' appeal, we argued that victims of human rights abuses enabled by powerful surveillance technologies must be able to seek redress through U.S. courts against both foreign and domestic corporations.

NSO Group notoriously manufactures "Pegasus" spyware, which enables full remote control of a target's smartphone. Pegasus attacks are stealthy and sophisticated: the spyware embeds itself into phones without an owner having to click anything (such as an email or text message). A Pegasus-infected phone allows government operatives to intercept personal data on a device as well as cloud-based data connected to the device.

Our brief highlights multiple examples of Pegasus spyware having been used by governmental bodies around the world to spy on targets such as journalists, human rights defenders, dissidents, and their families. For example, the Saudi Arabian government was found to have deployed Pegasus against *Washington Post* columnist Jamal Khashoggi, who was murdered at the Saudi consulate in Istanbul, Turkey.

In the present case, *Dada v. NSO Group*, the plaintiffs are affiliated with *El Faro*, a prominent independent news outlet based in El Salvador, and were targeted with Pegasus through their iPhones. The attacks on *El Faro* journalists coincided with their investigative reporting into the Salvadorian government.

The plaintiffs sued NSO Group in California because NSO Group, in deploying Pegasus against iPhones, abused the services of Apple, a California-based company. However, the district court dismissed the case on a *forum non conveniens* theory, holding that California is an inconvenient forum for NSO Group. The court thus concluded that exercising jurisdiction over the foreign corporation was inappropriate and that the case would be better considered by a court in Israel or elsewhere.

However, as we argued in our brief, NSO Group is already defending two other lawsuits in California brought by both Apple and WhatsApp. And the company is unlikely to face legal accountability in its home country—the Israeli Ministry of Defense provides an export license to NSO Group, and its technology has been used against citizens within Israel.

That's why this case is critical—victims of powerful, increasingly-common surveillance technologies like Pegasus spyware must not be barred from U.S. courts.

As we explained in our brief, the private spyware industry is a lucrative industry worth an estimated $12 billion, largely bankrolled by repressive governments. These parties widely fail to comport with the United Nations' *Guiding Principles on Business and Human Rights*, which caution against creating a situation where victims of human rights abuses "face a denial of justice in a host State and cannot access home State courts regardless of the merits of the claim."

The U.S. government has endorsed the *Guiding Principles* as applied to U.S. companies selling surveillance technologies to foreign governments, but also sought to address the issue of spyware facilitating state-sponsored human rights violations. In 2021, for example, the Biden Administration

recognized NSO Group as engaging in such practices by placing it on a list of entities prohibited from receiving U.S. exports of hardware or software.

Unfortunately, the *Guiding Principles* expressly avoid creating any “new international law obligations,” thus leaving accountability to either domestic law or voluntary mechanisms.

Yet voluntary enforcement mechanisms are wholly inadequate for human rights accountability. The weakness of voluntary enforcement is best illustrated by NSO Group supposedly implementing its own human rights policies, all the while acting as a facilitator of human rights abuses.

Restraining the use of the *forum non conveniens* doctrine and opening courthouse doors to victims of human rights violations wrought by surveillance technologies would bind companies like NSO Group through judicial liability.

But this would not mean that U.S. courts have unfettered discretion over foreign corporations. The reach of courts is limited by rules of personal jurisdiction and plaintiffs must still prove the specific required elements of their legal claims.

The Ninth Circuit must give the *El Faro* plaintiffs the chance to vindicate their rights in federal court. Shielding spyware companies like NSO Group from legal accountability does not only diminish digital civil liberties like privacy and freedom of speech—it paves the way for the worst of the worst human rights abuses, including physical apprehensions, unlawful detentions, torture, and even summary executions by the governments that use the spyware.

Join EFF Lists

Previous Chapter Next Chapter