LAWFARE

CYBERSECURITY

Summary: WhatsApp Suit Against NSO Group

By Erik Manukyan Thursday, November 7, 2019, 3:12 PM

DayZero: Cybersecurity Law and Policy

WhatsApp, which is owned by Facebook, filed a complaint on Oct. 29 in the U.S. District Court for the Northern District of California against Israeli cyberintelligence company NSO Group Technologies, asserting that NSO Group spyware had been used to infect 1,400 cell phones with the purpose of surveilling the communications of a target class of WhatsApp users.

This lawsuit comes on the heels of a number of news stories linking NSO Group technology to state-sponsored campaigns against human rights activists and journalists, such as Jamal Khashoggi, who is widely considered to have been targeted with NSO software by the Saudi government. In an op-ed published by the Washington Post on the same day WhatsApp filed its lawsuit, the head of WhatsApp, Will Cathcart, decried NSO Group's alleged complicity in targeting "100 human-rights defenders, journalists and other members of civil society across the world." In light of these abuses, Cathcart concluded that proprietary surveillance technologies that "enable surveillance into our private lives," such as NSO Group's, "are being abused, and the proliferation of this technology into the hands of irresponsible companies and governments puts us all at risk."

Moving beyond his narrow grievances with NSO Group's particular conduct, Cathcart offered four prescriptions for how to best protect data privacy going forward. First, Cathcart asserted that "technology companies should never be required to intentionally weaken their security systems." WhatsApp has argued this point for years as it fights the mandatory introduction of a backdoor to the end-to-end encryption typical of data sent on its application. Second, Cathcart called on technology firms to cooperate in the promotion of human rights, specifically, the right to privacy. To Cathcart, tech companies should share information and partner with security researchers in order to "build[] safer systems" that will shield dissident voices from the governments that seek to suppress them. Third, Cathcart implored technology companies not to target each other in cyberattacks and to refrain from selling technology to actors who seek to use these tech products to exploit companies' vulnerabilities. Fourth, asserting that "more needs to be done" regarding the oversight of cyberweapons, Cathcart exhorted tech firms to "join" U.N. Special Rapporteur David Kaye in calling for an "immediate moratorium on the sale, transfer and use of dangerous spyware."

This op-ed shed light on WhatsApp's normative vision for a more data-protective digital environment while criticizing NSO Group for violating that same vision. But the real bite of the op-ed was in the subtext—from now on, companies that choose to violate these norms will be slammed with litigation.

WhatsApp Complaint in Federal Court

WhatsApp alleges that NSO Group deployed Pegasus, one of several spyware technologies developed and operated by the surveillance company, on 1,400 mobile devices operating the WhatsApp mobile application.

Pegasus and NSO Group Background

Pegasus is a remote-access Trojan that first appears on mobile devices as an innocuous communication. Before the spyware can infect the device, a mobile device user must install the spyware. However, this installation is often commenced inadvertently, sometimes even without the mobile device user's input. For example, NSO Group has allegedly used spear-phishing—the process of targeting a specific user with a fraudulent email, message or link outfitted to appear as if it were from a reputable company—to achieve remote installation. Once a mobile user opens the sham message or clicks the link, Pegasus "surreptitiously" installs on the mobile device, ultimately giving NSO Group customers—both legitimate and malicious government actors—access to data contained on the target device.

According to WhatsApp, Pegasus could remotely extract data and intercept communications from a host of communications applications such as "iMessage, Skype, Telegram, WeChat, Facebook Messenger, WhatsApp, and others." WhatsApp suspects that Pegasus was "modular malware," meaning it could be "customized" for multiple uses on the same phone. WhatsApp believes that this modularity enabled Pegasus to "intercept communications, capture screenshots, and exfiltrate browser history and contacts" from devices.

The suit claims that NSO Group facilitated and oversaw data extraction by its customers. The group achieved this by using a central network to update Pegasus spyware installed on various target devices, by sending data between target devices and NSO Group customers' devices, and even by imposing caps on the number of devices its customers were permitted to infect with Pegasus.

WhatsApp's Alleged Legal Injury

WhatsApp asserts that, between January 2018 and May 2019, NSO Group created several WhatsApp accounts that were then used to send "malicious code" to 1,400 target devices. According to WhatsApp, NSO Group was able to do this by "reverse-engineer[ing]" the WhatsApp application. This allowed NSO Group to emulate typical WhatsApp network traffic and pass this code undetected. This code was transmitted under the guise of a regular phone call, and, regardless of whether WhatsApp users answered the deceptive phone call or let it ring, the code was embedded in the receiving devices' memories. After this initial breach, NSO Group allegedly used WhatsApp servers to transmit encrypted data packets designed to trigger the extraction code on target devices. Once triggered, the code would connect to NSO Group servers, established for the purpose of downloading and installing malware onto the target devices. From that point forward, NSO Group and NSO Group customers had access to the data contained on these target devices.

Based on these facts, WhatsApp alleges four causes of action for legal remedy: the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; the California Comprehensive Computer Data Access and Fraud Act, California Penal Code § 502; breach of contract; and trespass of chattel. NSO Group's conduct, WhatsApp argues, "interfered with the WhatsApp Service[,]" "burdened" its "computer network[,]" and injured WhatsApp's "reputation, public trust, and good will."

Though NSO Group has previously been sued by individual victims of its spyware, WhatsApp's lawsuit marks the first time NSO Group has been sued by a technology company whose users were targeted by the Israeli company. WhatsApp's legal complaint ventures into new territory in data privacy litigation. If WhatsApp is successful in court, other technology companies may be similarly emboldened to pursue legal remedies against companies like NSO Group that are facilitating cyberattacks on mobile device users.

Topics: Cybersecurity

Tags: Facebook, lawful hacking, Encryption

Erik Manukyan is a second-year student at Harvard Law School, where he is a Principal Senior Editor on the National Security Journal. He graduated from the University of California, Los Angeles with a B.A. in Political Science.