WhatsApp's Case Against NSO Group Hinges on a Tricky Legal Argument

Andy Greenberg ⋮ 8-10 minutes ⋮ 10/29/2019

WhatsApp just took a hard new line against the malware industry, suing notorious Israeli surveillance contractor NSO Group for attacks on more than a thousand of its users. The case could mark a turning point in Silicon Valley's fight against private-sector espionage mercenaries. But before it can convince a court that NSO engaged in criminal hacking, WhatsApp may have to win a thorny legal argument—one that legal experts say could require some creative contortions.

On Tuesday afternoon, WhatsApp published a statement accusing NSO of targeting 1,400 of its users, including at least 100 members of "civil society" such as journalists and human-rights defenders, with malicious voice calls designed to infect targeted phones with malware and steal messages despite WhatsApp's end-to-end encryption. Those numbers would represent a new scale for NSO, whose malware has already been linked to attacks against activists ranging from the now-imprisoned United Arab Emirates dissident Ahmed Mansoor to Mexican activists opposing a soda tax.

WhatsApp paired its statement with a lawsuit in a Ninth Circuit court, accusing NSO of violating the Computer Fraud and Abuse Act, as well as state-level charges including breach of contract and interfering with their property. The case represents a bold attempt to use the CFAA in an unusual way: to punish not just hackers who breach a company's computers, but those who exploit its software to breach the computers of its users.

But some hacking-focused lawyers who have analyzed WhatsApp's complaint warn that—noble as its attempt to slap back NSO and protect its users may be—its central argument may not fly in court.

That's because, fundamentally, the CFAA outlaws so-called "unauthorized access," explains Tor Ekeland, a well-known hacker defense attorney. To make that charge stick, WhatsApp will have to show that NSO obtained illegal access to WhatsApp's own systems. Given that NSO's targets were WhatsApp users rather than, say, WhatsApp's servers, they'll have to find an argument that they, as the plaintiff, were the victim. "The fundamental question is, what's the unauthorized access?" says Ekeland. "You might be able to argue that NSO hacked WhatsApp and not just their users. Maybe they're trying to make that argument. But they're not being clear about it, and that lack of clarity is an attack vector for the defendant."

WhatsApp's most obvious unauthorized access argument relates to its terms of service, which prohibit reverse-engineering WhatsApp's code, harming its users, or sending malware via WhatsApp. The company might argue that by agreeing to those terms of service and then violating them, NSO's use of WhatsApp was unauthorized all along. The complaint appears to lay the groundwork for that case: It points out that NSO Group staff "created various WhatsApp accounts and agreed to the WhatsApp Terms."

But that terms-of-service argument will be an uphill battle, says Ekeland. Terms of service have long been a controversial element of hacking cases, from the 2009 cyberbullying case of Lori Drew to the hacking charges against information freedom activist Aaron Swartz. And the Ninth Circuit in particular has set a clear precedent that terms-of-service violations alone don't constitute unauthorized access. "A terms of service violation under the CFAA is a very thin reed to hang your case on," Ekeland says.

WhatsApp parent company Facebook has sought out CFAA rulings against terms-of-service violators in the past. It sent a warning to a company called Power Ventures, which created its own user interface for Facebook and other social media sites, to stop violating its terms. It then sued under the CFAA only after the company persisted. In that instance, a judge ruled explicitly that Power Ventures had broken the CFAA—but that it wouldn't have if Facebook hadn't first told it to stop accessing its site.

"There's a lot of precedent here with Facebook," says Alex Stamos, former Facebook chief security officer. "If you use Facebook services in the way where you are knowingly violating terms of services, they can bar you from the service and call it a violation of the CFAA."

But WhatsApp's lawsuit doesn't make any mention of prior notice to NSO to stop abusing its services or hacking its users. "I don't see anything that says they sent a case and desist or attempted to block them," says Riana Pfefferkorn, associate director of surveillance and cybersecurity at Stanford Law School's Center for Internet and Society. "Absent more, they won't be able to hook the CFAA violation on the terms of service."

Another, trickier strategy for WhatsApp may be to claim that the malicious data NSO sent via WhatsApp servers *was itself* a kind of unauthorized access. The WhatsApp complaint accuses NSO of initiating malicious calls that hid their attack code in fake settings data, and in doing so bypassed "technical restrictions" on what sort of data WhatsApp's servers were designed to pass on to phones. This may be the crux of WhatsApp's CFAA claim: that WhatsApp's own access restrictions were "hacked" with this technique, just as if someone had bypassed a more obvious access restriction like one that demanded a username and password. "There might be a way to argue that NSO concealing its malware as normal traffic is actually a hack," says Ekeland.

But that appears to be an untested argument, and one that will require some creative logic to explain to a judge or jury. "They're saying 'you used our system in a way we didn't want you to,'" Ekeland says. "But no one hacked a username or password."

When WIRED reached out to WhatsApp, a spokesperson declined to comment—beyond cryptic clues—on the company's legal strategy. "This is a not a typical CFAA case," the spokesperson said. "We look forward to explaining more in court as we go forward."

Even if the courts were to dismiss WhatsApp's CFAA charge, NSO would still face three other charges, including California state hacking charge and breach of contract. But all of those other allegations, Ekeland points out, are based on state laws, which would mean the case would need to be refiled in state court. And all eyes will be on the CFAA dispute, in particular, because it could mean NSO is liable for criminal hacking charges as well. "The CFAA is the main show," says Stanford's Riana Pfefferkorn.

"We dispute today's allegations and will vigorously fight them," said NSO in a statement. "The sole purpose of NSO is to provide technology to licensed government intelligence and law enforcement agencies to help them fight terrorism and serious crime. Our technology is not designed or licensed for use against human rights activists and journalists."

Beyond its legal strategy, WhatsApp may have already scored a different sort of win, Pfefferkorn points out. It has revealed, in dramatic fashion, the extent of NSO's alleged hacking. And by simply posing the question of whether the company's surveillance has broken US law, it's scored a significant PR coup against an infamous hacking crew—one that may put the company on its back foot.

"Part of this is a publicity exercise calling out NSO, which has a terrible track record of targeting journalists, activists, and human rights defenders," Pfefferkorn says. "Potentially they're trying to up the embarrassment factor for NSO and other zero-day vendors and hackers for hire. There's a name and shame element to this." Even if the charges don't stick, the shame may not be so easy to wash away.

More Great WIRED Stories

- Inside Apple's high-flying bid to become a streaming giant
- Can license plate readers really reduce crime?
- The acid sludge streaming out of Germany's coal mines
- *Ripper*—the inside story of the egregiously bad videogame
- Tired of jet lag? This app will help reset your clock
- 👁 Prepare for the deepfake era of video; plus, check out the latest news on AI
- 🎧 Things not sounding right? Check out our favorite wireless headphones, soundbars, and Bluetooth speakers