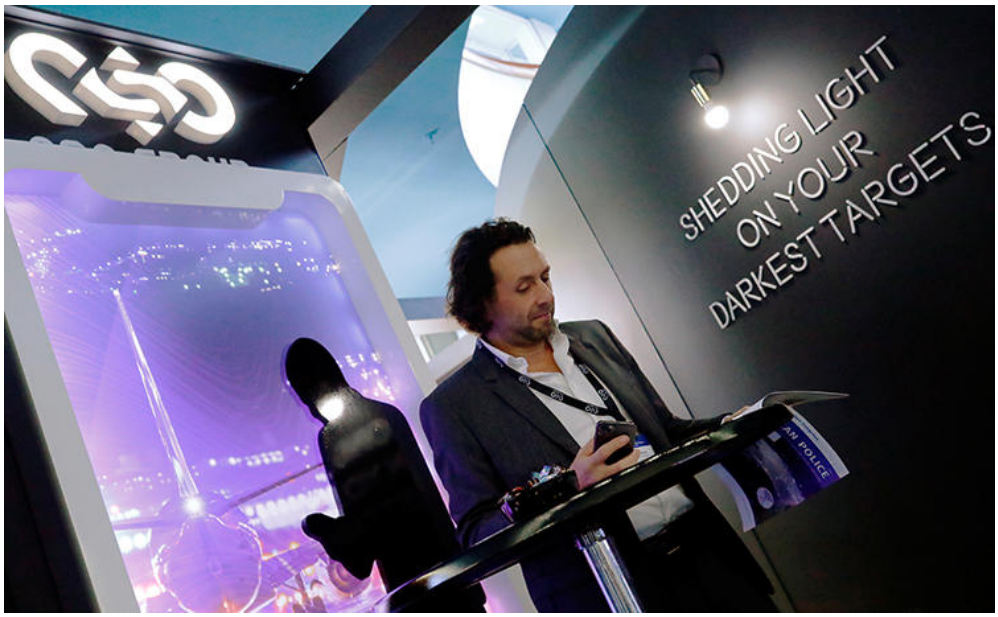

A man reads at a stand of the Israeli technology firm NSO Group at the annual European Police Congress in Berlin, Germany, February 4, 2020. WhatsApp has alleged the group's technology enabled the remote surveillance of members of civil society via their phones, with several Indian journalists among the targets. (Reuters/Hannibal Hanschke)

After WhatsApp spyware allegations, Indian journalists demand government transparency

By Avi Asher-Schapiro/CPJ Global Tech Senior Correspondent on February 24, 2020 9:06 AM EST

In the summer of 2019, Saroj Giri was preparing a lecture on the panopticon—an 18th century system to surveil an entire prison from a single viewpoint—when a message lit up his phone. It was from WhatsApp, warning Giri that someone had tried to hack the popular messaging app to spy on his cell phone remotely.

The irony was not lost on Giri, a University of Delhi lecturer who has criticized India's political class as a commentator for several local publications. "They were putting the panopticon on me," he told CPJ by phone. He suspects his phone was successfully hijacked, he said, though he can't be sure who—or what institution—was responsible.

News website *Scroll.in* listed nearly two dozen people in India who reported getting similar notifications. In October 2019, WhatsApp, which is owned by Facebook, sued the Israeli technology firm NSO Group in a United States federal court and accused the company of exploiting a vulnerability in WhatsApp to enable its clients to spy on at least 100 members of civil society around the world. The NSO Group disputed the allegations "in the strongest possible terms" in a statement at the time, on the grounds that it only sells technology to governments to combat terrorism and serious crime.

Giri is one of five Indian journalists and commentators CPJ spoke with from the list of self- reported targets. All told CPJ of pressure they have faced because of something they have published; some said the WhatsApp notification came in conjunction with intimidation or other reprisals from the government for their work. All five denied any involvement in terrorism or serious crimes. They told CPJ that the sophistication of the technology reportedly involved in the attack, and the lack of recourse available to them under Indian law, has left them shaken.

"We were not prepared for this kind of an attack," Giri told CPJ. "You know what we were prepared for? The kind of attacks where the police come knocking at your door."

While it's not clear which national or state agencies, if any, could have deployed the spyware, experts interviewed by CPJ said the government's efforts to investigate WhatsApp's accusations have been half-hearted at best, while the NSO Group has taken no public steps to remedy the alleged abuse. The incident highlights the lack of transparency around the Indian government's surveillance powers, a concern that has escalated under Prime Minister Narendra Modi and the ruling Bharatiya Janata Party (BJP); during a recent trip across India, CPJ found the press "much more controlled under Modi's administration than previous ones."

CPJ reached out to India's IT Ministry and the Home Ministry—which oversees law enforcement and intelligence matters—for comment on the WhatsApp suit and the alleged surveillance of journalists, but did not receive a reply.

The NSO Group—which was acquired last year by the British private equity firm Novalpina Capital—did not respond to CPJ's requests for interview or to questions about its clients in India sent by email in early 2020.

"The perception is that the government is monitoring what you are saying publicly—and what you say privately. That's going to make journalists be more careful," Raman Chima, the Delhi-based senior international counsel for the digital rights group Access Now told CPJ. A digital security helpline run by the group has seen a recent uptick in requests from journalists in India concerned about surveillance, he said

"When the people we work with find out about this, they may not want to keep in touch with us," Shubhranshu Choudhary told CPJ. Choudhary, who is based in Chhattisgarh state, runs CGNet Swara, a voice-based online portal that allows people to report local news via cell phone. He was notified by WhatsApp that he was targeted in late 2019; like the other people CPJ spoke with, he doesn't know why, or whether the attack was successful. But he said

his work promoting citizen journalism among tribal people, who are locked in a land dispute with authorities, may have upset the powers that be. “All our meetings happen on WhatsApp,” he said.

Not all of the victims who received a notification understood why they would merit such an apparently expensive and advanced operation. “I don’t know why I was targeted,” Sidhant Sibal, the Delhi-based diplomatic correspondent for the private Indian TV news station WION, told CPJ in 2019. “I’m not that big of a guy. I’m actually a no-one.”

For leading Indian digital rights lawyer Mishi Choudhary, though, the targeting of any reporter affects the entire journalism community. “People start wondering, is there a problem with my phone?” she told CPJ.

Some of the targets interviewed by CPJ reported being followed and menaced by security forces in real life, making the WhatsApp attack just part of their extensive surveillance experience. Seema Azad edits the bi-monthly politics magazine *Dartak* in Uttar Pradesh, which has criticized several BJP policies as anti-Muslim, she told CPJ. She suspects she has been under surveillance for years, she said, ever since she was jailed for sedition, as CPJ noted in 2012. Her sources have become wary since news of the WhatsApp suit broke, she said, and officials who contribute to *Dartak* pseudonymously are now unwilling to send her anything by phone.

Another target, Anand Teltumbde, has published widely on rights for Dalits, a group that’s long been oppressed within India’s caste system, and faced harassment and legal action that Human Rights Watch and Amnesty International India have condemned.

“I have been writing for many years now—and I have been critical, harshly critical of successive Indian governments,” Teltumbde told CPJ. “This government has gone berserk.”

Former home secretary: NSO products ‘available and used’ by Indian authorities

Gopal Krishna Pillai, who served as home secretary under a Congress Party government between 2009 and 2011 before leaving politics, told CPJ that NSO products are “available and used” by authorities in India, but did not respond to a request to identify the agencies involved. Pillai has told Indian media he was aware of several thousand Indians targeted for surveillance under his tenure. Pillai told CPJ that he believes the current regime is spying more aggressively.

“What journalists write comes under stricter scrutiny,” he said. And journalists with an “anti-government slant” have “invited adverse action” from the government, he said, without elaborating.

As of February 2020, Modi’s government had yet to respond to a letter from 19 of the people affected by the breach asking about its dealings with NSO Group, Shubhranshu Choudhary, who was a signatory, told CPJ. An official statement in October 2019 called reports of the hack “misleading,” and part of an attempt to “malign the government.” In parliament, IT Minister Ravi

Shankar Prasad did not confirm or deny whether his government had conducted business with the NSO Group. “To the best of my knowledge, no unauthorized interception has been done,” local news reports cited him as saying.

Mishi Choudhary told CPJ that the BJP government inherited a legal framework which grants authorities surveillance powers with little to no oversight. The Software Freedom Law Center, an organization she founded, obtained data in 2014 showing that India’s central government was issuing more than 100,000 phone interceptions orders per year, data the government no longer releases, she said.

“Phone tapping is considered extremely common,” Rohan Venkataramakrishnan, the associate editor of *Scroll.in,* told CPJ. “Anyone reporting on senior government officials or politicians takes it as a given.”

Encrypted services like WhatsApp felt more private, according to Venkataramakrishnan. “The news of the WhatsApp hack was quite jarring,” he said. The attack used a “zero-click vulnerability,” *The New Yorker* reported, meaning an attacker could infect a device by placing a WhatsApp voice call, whether or not the target answered.

NSO products were designed to help government intelligence and law enforcement agencies trace criminals who are “‘going dark’ through the use of encrypted communications,” in the words of a 2019 press release from Novalpina Capital.

“It used to be like looking for a needle in a haystack,” said Mishi Choudhary. “But with NSO, it’s much more targeted.”

Shashi Tharoor, a member of parliament with the opposition Congress Party, chairs a government committee tasked with probing the alleged surveillance. In a February interview, he told CPJ that the technology involved is hugely expensive. “It’s not the amount that could be authorized by a junior official,” he said. Leaked documents analyzed by *The New York Times* in 2016 suggest that the NSO Group has charged over $650,000 to spy on 10 iPhones.

Tharoor has accused Om Birla, BJP speaker of the lower house of parliament, of trying to block the committee from meeting. “I am afraid every step on this issue is going to be a challenge,” Tharoor said. “And when I prepare a report there will be resistance.” CPJ requested comment from Birla, but did not receive a reply before publication.

The Congress Party-led state government in Chhattisgarh conducted a separate inquiry, after a number of victims were identified in the state, and anonymous government sources told the Delhi-based *Sunday Guardian* newspaper and other outlets that the NSO Group had made a presentation to senior police officers there.

The state’s probe could not link government officials with the alleged attacks, according to the *Hindustan Times*. Shubhranshu Choudhary told CPJ he was not impressed with the investigation. “The questions were very basic,” he said.

CPJ contacted Taran Sinha, director of the state's public relations department and a member of the investigative panel, and emailed a Chhattisgarh police spokesperson for comment. Neither responded before publication.

The NSO Group told CPJ in October 2019 that it "takes appropriate action" against clients who misuse its technology. After the alleged hacking took place in India—but before WhatsApp notified the targets—NSO announced a new policy to integrate "human rights due diligence" into its work, including "remedies culminating in the termination of use of our products after a substantiated case of severe misuse."

CPJ emailed an NSO Group spokesperson in 2020 to ask whether the alleged targeting of journalists in India constitutes misuse of its products and what remedies resulted, but received no response before publication.

"These abuses were taking place…even as NSO had told the world that it was under new management and that abuses were a thing of the past," John Scott-Railton, a senior researcher with the Citizen Lab research group at the University of Toronto, told CPJ. Citizen Lab says it has detected NSO technology in 45 different countries—including India—and documented Mexican and Saudi journalist targets in addition to the victims of the WhatsApp hack, which the group helped investigate.

"While it is imperative for companies to have human rights policies, it is impossible to gauge their commitment to enforce them without real transparency," David Kaye, the U.N. Special Rapporteur for freedom of opinion and expression, told CPJ in February. Kaye called for a moratorium on trade and deployment of commercial spyware in a June 2019 report that named the NSO Group's product Pegasus as "a paradigmatic example."

In India, in the absence of a credible investigation or legal redress, journalists are left to assume phones can be compromised at any time. But targets like Giri are increasingly keen to press for transparency. "We need whistleblowers in this country," he said. "We need to know what they are really up to."

For information on digital safety, consult CPJ's Digital Safety Kit.

Kunal Majumder, CPJ's India correspondent in New Delhi, contributed reporting.

Avi Asher-Schapiro is CPJ's Global Tech Senior Correspondent. He is a former staffer at VICE News, International Business Times, and Tribune Media, and an independent investigative reporter who has published in outlets including The Atlantic, The Intercept, and The New York Times.

CPJ is a 501(c)3 non-profit.
Our EIN is 13-3081500.
Committee to Protect Journalists
P.O. Box 2675
New York, NY 10108