Committee to Protect Journalists

An independent, nonprofit organization that promotes press freedom worldwide.
We defend the right of journalists to report the news safely and without fear of reprisal.

Spyware and Press Freedom

Key points

- Spyware, once reserved for spies and hackers, can control a journalist's phone and download its contents.
- Government actors are purchasing and using spyware without public accountability – even in countries where journalists face arrest and murder for their work.
- Companies develop and sell commercial spyware without sufficient regulation or transparency to prevent abuse.
- Immediate action by governments and companies is necessary to slow proliferation and wrongful use of spyware against the press.

What is spyware?

Spyware is designed to enable secret, unauthorized access to an electronic device without being detected. It can be used to seize control of a journalists' phone or computer, potentially exposing where they are, the identity of their sources, their private conversations, and more.

Some spyware tools infect a target's phone via spoof messages that look legitimate and trick the recipient into clicking on a malicious link. Others can access a target's device without their taking any action.

The scope of the problem

Governments use spyware for national security, intelligence, and law enforcement efforts, many of which may be legitimate. But the same technology is being used to target journalists writing about the United Arab Emirates, Saudi Arabia, Morocco, Ethiopia, Mexico, and India, among others, CPJ has found.

While hackers and spy agencies may create or trade surveillance tools in secret, companies based in Europe, the U.S. and Israel openly develop and market spyware to government clients worldwide.

Though companies don't discuss specific contracts publicly, some say they vet those clients and investigate allegations that their products are being abused. Yet this has done nothing to slow the reports of abuse.

Why it matters

Journalists rely on mobile phones, computers, and internet networks to track breaking news, communicate with sources and colleagues, and publish stories. Spyware threatens their ability to do so privately and securely.

Journalists have told CPJ they fear they – or their sources – could be compromised or harmed following a spyware attack, causing concern that targeted surveillance is encouraging self-censorship.

If government officials can spy on the reporters investigating them without oversight or penalty, press freedom and the public's right to information are at risk.

Spyware: Pegasus

SOLD BY: NSO Group

LOCATION: Based in Israel, acquired by its management in 2019 with funding from the U.K. private equity firm Novalpina Capital.

ALLEGED TARGETS: The University of Toronto's Citizen Lab, which investigates spyware, say Pegasus has been use in multiple attempts to hack journalists and their associates, including:

- New York Times journalist Ben Hubbard in Lebanon, who covers Saudi Arabia;
- Colleagues of Mexican journalist Javier Valdez, who was killed for his work in 2017 – as well as his wife, Griselda Triana;
- Saudi dissident Omar Abdulaziz, a Canadian permanent resident and confidante of Jamal Khashoggi, the Washington Post columnist murdered by Saudi operatives in 2018.
- The company's response: "We take the responsibility to ensure the proper use of our products very seriously and fully investigate any credible allegation of misuse."

Visit cpj.org/spyware for a link to their full statement and more alleged targets of Pegasus and other tools.

Recommendations

Governments and intergovernmental bodies have taken some steps to address the unregulated proliferation of spyware and its wrongful use. In 2019, the UN special rapporteur on freedom of opinion and expression issued a report proposing a legal and policy framework for regulation, accountability and transparency within the private surveillance industry. In 2020, the U.S. State Department issued guidance for companies, though it is not binding.

The European Union has separately agreed on export control regulations for surveillance technology which, once enacted, will promote transparency, but represent only the minimum EU member states and companies must do to prevent abuse, according to an analysis by CPJ and other groups.

As a result, there still remain few effective barriers preventing governments with demonstrated histories of surveilling and curtailing the free press from acquiring sophisticated surveillance technology.

It is essential that governments and companies act immediately to stop the abuse of spyware against journalists. The Committee to Protect Journalists makes the following policy suggestions.

For governments

- Adopt and enforce legislation to:
  - bar the use of spyware to surveil journalists and media outlets;
  - bar the export or transfer of surveillance technology and expertise to governments with poor press freedom records, including via third parties;
  - bar state agencies from purchasing or licensing the export of surveillance technology from companies that sell to governments with poor press freedom records, or that lack mechanisms to prevent their clients from targeting the press in line with the UN Guiding Principles on Business and Human Rights.
- Establish independent oversight of state-supported use of spyware and hacking tools and enable accountability and remedy in documented cases of abuse against the media.
- Sanction actors who have spied or facilitated spying on journalists through the sale or use of spyware.
- Require public reporting and consultation about surveillance purchases and exports.
- Document the abuse of surveillance technology against journalists in government human rights reports.

For companies

- Make a public commitment to press freedom and protecting journalists and media outlets from covert surveillance.
- Prohibit clients from spying on journalists in explicit terms in contracts and licenses.
- Revoke access to spyware when abuse is detected, and report abuse to affected individuals and relevant authorities and oversight bodies.
- Establish procedures to review complaints and support human rights monitors investigating allegations of abuse involving specific products.

To speak with a CPJ representative about these recommendations, please contact:

Gypsy Guillen Kaiser
Advocacy Director
gGuillenkaiser@cpj.org

Michael De Dora
Washington Advocacy Manager
mdedora@cpj.org

Tom Gibson
Brussels Advocacy Manager
tgibson@cpj.org