US to adopt new restrictions on using commercial spyware

March 27 2023, by Nomaan Merchant

A person types on a laptop keyboard in North Andover, Mass, June 19, 2017. The U.S. government will restrict its use of commercial spyware tools that have been used to surveil human rights activists, journalists and dissidents around the world, under an executive order issued Monday, Oct. 27, 2023, by President Joe Biden. Credit: AP Photo/Elise Amendola, File

The U.S. government will restrict its use of commercial spyware tools that have been used to surveil human rights activists, journalists and dissidents around the world, under an executive order issued Monday by President Joe Biden.

The order responds to growing U.S. and global concerns about programs that can capture text messages and other cellphone data. Some programs—so-called "zero-click" exploits—can infect a phone without the user clicking on a malicious link.

Governments around the world—including the U.S.—are known to collect large amounts of data for intelligence and law enforcement purposes, including communications from their own citizens. The proliferation of commercial spyware has made powerful tools newly available to smaller countries, but also created what researchers and human-rights activists warn are opportunities for abuse and repression.

The White House released the executive order in advance of its second summit for democracy this week. The order "demonstrates the United States' leadership in, and commitment to, advancing technology for democracy, including by countering the misuse of commercial spyware and other surveillance technology," the White House said in a statement.

Biden's order, billed as a prohibition on using commercial spyware "that poses risks to national security," allows for some exceptions.

The order will require the head of any U.S. agency using commercial programs to certify that the program doesn't pose a significant counterintelligence or other security risk, a senior administration official said.

Among the factors that will be used to determine the level of security risk is if a foreign actor has used the program to monitor U.S. citizens

without legal authorization or surveil human rights activists and other dissidents.

House Select Committee on Intelligence ranking member Rep. Jim Himes, D-Conn speaks during the committee's annual open hearing on worldwide threats, at the Capitol in Washington, March 9, 2023. Himes said in a committee hearing last year that commercial spyware posed a “very serious threat to our democracy and to democracies around the world.” He said Monday the new order would be a “critical tool" that should be followed by other democracies taking steps against spyware. Credit: AP Photo/Carolyn Kaster, File

"It is intended to be a high bar but also includes remedial steps that can be taken ... in which a company may argue that their tool has not been

misused," said the official, who briefed reporters on condition of anonymity under White House ground rules.

The White House will not publish a list of banned programs as part of the executive order, the official said.

John Scott-Railton, a researcher at the University of Toronto's Citizen Lab who has long studied spyware, credited the Biden administration for trying to set new global standards for the industry.

"Most spyware companies see selling to the U.S. as their eventual exit path," Scott-Railton said. "The issue is the U.S. until now hasn't really wielded its purchasing power to push the industry to do better."

Congress last year required U.S. intelligence agencies to investigate foreign use of spyware and gave the Office of the Director of National Intelligence the power to ban any agency from using commercial programs.

Rep. Jim Himes of Connecticut, the top Democrat on the House Intelligence Committee, said in a committee hearing last year that commercial spyware posed a "very serious threat to our democracy and to democracies around the world." He said Monday the new order should be followed by other democracies taking steps against spyware.

"It's a very powerful statement and a good tool, but alone it won't do the trick," he said.

A logo adorns a wall on a branch of the Israeli NSO Group company, near the southern Israeli town of Sapir, Aug. 24, 2021. The best known example of spyware, the Pegasus software from Israel's NSO Group, was used to target more than 1,000 people across 50 countries, according to security researchers and a July 2021 global media investigation, citing a list of more than 50,000 cellphone numbers. The U.S. has already placed export limits on NSO Group, restricting the company's access to U.S. components and technology. Credit: AP Photo/Sebastian Scheiner, File

Perhaps the best known example of spyware, the Pegasus software from Israel's NSO Group, was used to target more than 1,000 people across 50 countries, according to security researchers and a July 2021 global media investigation, citing a list of more than 50,000 cellphone numbers. The U.S. has already placed export limits on NSO Group, restricting the

company's access to U.S. components and technology.

Officials would not say if U.S. law enforcement and intelligence agencies currently use any commercial spyware. The FBI last year confirmed it had purchased NSO Group's Pegasus tool "for product testing and evaluation only," and not for operational purposes or to support any investigation.

White House officials said Monday they believe 50 devices used by U.S. government employees, across 10 countries, had been compromised or targeted by commercial spyware.

Despite NSO's assertions that the program is supposed to be used to counter terrorism and crime, researchers found the numbers of more than 180 journalists, 600 politicians and government officials, and 85 human rights activists.

Pegasus use was most commonly linked to Mexico and countries in the Middle East. Amnesty International has alleged Pegasus was installed on the phone of Jamal Khashoggi's fiancée just four days before the journalist was killed in the Saudi consulate in Istanbul in 2018. NSO has denied the allegation that its software was used in connection with Khashoggi's murder.

The family of Paul Rusesabagina, credited with saving more than 1,200 lives during the Rwandan genocide, a story depicted in the movie "Hotel Rwanda," has also alleged it was targeted by spyware. Rusesabagina was lured back to Rwanda under false pretenses and jailed on terrorism charges before his release last week. Rwanda has denied using commercial spyware.