Andrew Napolitano on Pegasus & Predator Spy Systems: The Feds and Their Copycats

Andrew Napolitano on Pegasus & Predator Spy Systems: The Feds and Their Copycats

The Feds and Their Copycats

by **Andrew P. Napolitano**, *Judge Napolitano*
May 18, 2023

The federal government recently revealed that at least 50 U.S. government personnel working in 10 foreign countries have had their mobile devices hacked by unknown persons who employed software known as "zero-click." The zero-click product, called Pegasus, is manufactured by an Israeli high-tech company, called NSO Group.

Pegasus enables the user to download the contents of the target's mobile device or desktop without having to trick the target into clicking onto a link. It also enables the user to follow the person in possession of the device, capturing all texts and emails, as well as listening to conversations on the device or that take place in near proximity to it.

Pegasus is so sophisticated that its victims are largely unaware of the digital attack on their devices. The feds learned that they have been victimized by this software when Apple informed them. Apple told the feds to expect much more of this. The feds are deeply troubled by this warning, as they don't know who the victims are. The president himself was recently in Ireland, where his personal phone may have been targeted.

But don't feel sorry for the feds. They have been using this software and similar products on unsuspecting Americans since the Trump administration.

Here is the backstory.

In reply to a routine Freedom of Information Act request made in 2020, the FBI acknowledged spending $5 million to license Pegasus from NSO Group. When FBI director Christopher Wray was asked about this, he reluctantly told Congress that his agents bought zero-click, but he denied its use in law enforcement. What does that mean? Isn't the essence of the FBI's work law enforcement?

Wray claimed that the FBI only purchased zero-click in order to reverse engineer it — basically to see how it worked. But that's not truly why the FBI wanted Pegasus. It hoped to use the software to spy on Americans without first obtaining search warrants.

The Fourth Amendment to the U.S. Constitution, written in the aftermath of British searches of colonial homes not based on evidence of crimes, requires judicially issued search warrants based on probable cause of crime for all searches and seizures.

Thus, the owners and users of mobile devices and desktops — that's nearly every American — have a privacy right in the use of their devices and in the data they have stored in them. Even a narrow interpretation of the amendment that guarantees privacy in "persons, houses, papers, and effects" must acknowledge that a computer chip — the heart of every computer — is an "effect," and thus its owner or user enjoys privacy protection.

Protection from whom? Let's see.

When President Joe Biden learned of the FBI's use of Pegasus — the FBI secretly bought it during the Trump years — and the

FBI's shady explanation for its use of it, the White House announced an executive order that it claimed would prevent future use of zero-click. The Biden executive order stops the sales of Pegasus to Americans and to the government, but it does not stop the sales of all zero-clicks.

Rather than simply banning zero-click, rather than banning all warrantless searches, Biden banned only the use of one brand of zero-click software and only when it has also been used by foreign governments to target the U.S. government, when it is under the control of a foreign government, when it has been used to target the freedom of expression of foreign human rights activists or when it has been used by foreign authoritarians.

What about stopping the use of zero-click by federal authoritarians? Biden banned it because of how others use it, not because, in its essence, it violates the Fourth Amendment. Quick to pick up on this, the feds quickly purchased Predator — a twin of Pegasus, made by another foreign high-tech firm, with a more benign track record of sales and use.

What good does Biden's executive order do? Whom does it protect? The Biden executive order is Joe Biden at his worst. Claiming to deny commercial benefit to a foreign company because it also sells to bad guys but permitting another foreign company to sell functionally the same product to the feds protects no one's Fourth Amendment rights.

When Thomas Jefferson predicted shortly before he died in 1826 that, in the long run, personal liberty would shrink and government power would grow, he could not have imagined any of this. It seems that, no matter who is in the White House and which political party controls either house of Congress, the tentacles of government reach deeper into our lives with every tick of the clock.

Is there any area of private or harmless behavior that the

government leaves alone?

The government that Jefferson left us has been inverted. That government needed the permission of the voters to do nearly anything. Today, we need the permission of the government to do nearly everything. And folks under observation change on account of the observation.

Two of my closest friends — husband and wife — told me they were discussing diamond earrings on their cellphones with each other last week. Soon, ads for diamond earrings began popping up on their desktops.

This was obviously not the government, yet, government sets the tone and the standard. Federal agents use zero-click to hack into our computers because that's a lot easier than developing probable cause of crime and presenting it to a judge. Big tech uses hacking because that's more effective than advertising.

Now big tech targeting consumers can mimic the feds — and, like the feds, get away with it because when the government breaks its own laws, it sets a precedent for others to follow. Is this the government the Framers left us? Is it the government we voted for? What awaits us on the other side of this Orwellian landscape?

Connect with Andrew P. Napolitano

Cover image credit: geralt