Written by **Joe Wolverton, II, J.D.** on December 12, 2013

FBI Can Secretly and Remotely Activate Built-In Laptop Cameras

The National Security Agency (NSA) has no monopoly on the use of intrusive surveillance tools to keep us all under the watchful eye of government.

The *Washington Post* reports that an elite team of hackers employed by the Federal Bureau of Investigation (FBI) have developed an application that turns on built-in laptop cameras. According to details provided in the story, the software can be turned on remotely by the g-men and perhaps most notably, the little green light that typically signals a "live" camera is not illuminated when this application is in use.

In documents describing tactics uses by the FBI to track an elusive suspected terrorist threat named "Mo," a short history of the program is revealed.

> The FBI has been able to covertly activate a computer's camera — without triggering the light that lets users know it is recording — for several years, and has used that technique mainly in terrorism cases or the most serious criminal investigations, said Marcus Thomas, former assistant director of the FBI's Operational Technology Division in Quantico, now on the advisory board of Subsentio, a firm that helps telecommunications carriers comply with federal wiretap statutes.

Virtual hideouts are becoming increasingly rare as the federal government's hired hackers create increasingly sophisticated and surreptitious software, all with the aim of stretching the size of the surveillance net.

> The FBI's technology continues to advance as users move away from traditional computers and become more savvy about disguising their locations and identities. "Because of encryption and because targets are increasingly using mobile devices, law enforcement is realizing that more and more they're going to have to be on the device — or in the cloud," Thomas said, referring to remote storage services. "There's the realization out there that they're going to have to use these types of tools more and more."

Once "Mo" signed on to his Yahoo mail account, the spyware would be immediately activated and the feds could see anything within the sight of his built-in webcam. Incidentally, in a statement made to the *Washington Post*, Yahoo claimed it knew nothing of the operation and did not participate with the government in targeting one of its users.

Although this "network investigative technique" is shockingly invasive, it's not the first such furtive device used by the feds to watch and listen to citizens when they think they are safe from the prying eyes and eavesdropping ears of the federal government.

And, not only does the government have and use a variety of sophisticated surveillance techniques to watch us, but the courts continue to rubber stamp the legally suspect searches.

In the case of the FBI's tracking of "Mo," the *Washington Post* provides a summary of the agency's recourses to the courts for approval of its operation.

First, a "federal magistrate in Denver approved sending surveillance software to Mo's computer last year."

Notably, the authors of the *Post* story report on a similar surveillance request made before a judge in Houston that was rejected for being "extremely intrusive" and a likely violation of the Fourth Amendment's protections against unwarranted searches and seizures.

Next:

> Federal magistrate Judge Kathleen M. Tafoya approved the FBI's search warrant request on Dec. 11, 2012, nearly five months after the first threatening call from Mo. The order gave the FBI two weeks to attempt to activate surveillance software sent to the texan.slayer@yahoo.com e-mail address. All investigators needed, it seemed, was for Mo to sign on to his account and, almost instantaneously, the software would start reporting information back to Quantico.

After obtaining judicial approval, the FBI's hackers "would download the surveillance software to Mo's computer when he signed on to his Yahoo account."

Finally, the *Post* reports:

> The surveillance software was sent across the Internet on Dec. 14, 2012 — three days after the warrant was issued — but the FBI's program didn't function properly, according to a court document submitted in February.
>
> "The program hidden in the link sent to texan.slayer@yahoo.com never actually executed as designed," a federal agent reported in a handwritten note to the court.

This isn't the first time the federal bench has bowed to the wishes of the purveyors of the surveillance state. In fact, last year the court approved a petition by the federal government to deploy software that could be remotely downloaded to a cellphone, turning the device into a portable microphone without the user ever being the wiser.

In July 2012, the Ninth Circuit Court of Appeals ruled that agents of the federal government may use a cellphone as a microphone and record the conversations overheard even when the phone itself is not being used otherwise.

This frightening bit of judicial lawmaking came as part of the decision in the case of the *United States v. Oliva*, 2012 WL 2948542 (9th Cir. July 20, 2012).

For a bit of background, Oliva was convicted by a jury of drug-related crimes involving the distribution of methamphetamine, cocaine, and marijuana. He appealed a decision by a district court denying his motion to suppress evidence obtained from a series of electronic surveillance orders authorizing interception of communications over cellular phones associated with him and his alleged co-conspirators.

Oliva argued that the orders authorizing these wiretaps were not standard intercept orders and did not meet the "specificity" requirement of the applicable federal law.

In its decision, the Ninth Circuit upheld the lower court's ruling, essentially allowing the federal government to convert cellphones into "roving bugs" so long as the government makes it clear that it will be using the target's cellphone in that manner. Notice, the Ninth Circuit — a court created under the authority granted to Congress in Article III of the Constitution — did not throw out the matter as a violation of the defendant's Fourth Amendment right against "unreasonable searches and seizures." Instead, it simply informed the government that it needs to get permission before doing so.

There are, of course, far reaching implications of such a decision. As *The New American* reported last year, a person will not know, and perhaps will never know, if he has been the target of surveillance on the part of the federal government. Assuming, as many a savvy American would, that the federal government is liable to eventually want to monitor and record your personal electronic communication, is there not an expectation that when the cellphone is off the surveillance is suspended?

Not anymore. In the wake of the Ninth Circuit's ruling in *Oliva*, and the revelations regarding the FBI's ability to remotely control laptop cameras, "roving bugs" and secretly snooping webcams are likely to become a couple of the feds' favorite weapons in the ever-more sophisticated attacks on personal privacy.

A person's expectation of privacy when sitting at home talking to a friend is ridiculous in the face of the judicially upheld fact that government snoops may now use powerful surveillance technology to use your idle mobile phone as a very active mobile microphone.

At times such as this when the courts, Congress, and departments of the executive branch (the FBI, the NSA, and the Department of Homeland Security, among others) form an unholy alliance bent on obliterating the Constitution and establishing a country where every citizen is perpetually under the never-blinking eye of the government, it would be well to remember the words written by Alexander Hamilton in *Federalist*, No. 33.

In that letter, Hamilton explained that acts of the federal government exceeding its constitutional powers are not laws at all, but are "merely acts of usurpation, and will deserve to be treated as such."

There's no debate that the increasingly incredible intrusiveness of the federal government's surveillance programs exceeds any authority granted to it in the Constitution. As the *Washington Post* article rightly says:

> Online surveillance pushes the boundaries of the constitution's limits on searches and seizures by gathering a broad range of information, some of it without direct connection to any crime. Critics compare it to a physical search in which the entire contents of a home are seized, not just those items suspected to offer evidence of a particular offense.

The remedy is for state legislatures to uphold their obligation to stop all unconstitutional acts of the federal government at the state borders. They can accomplish this by enacting state statutes nullifying those acts, based on the 10th Amendment and their sovereign authority. On the other hand, should these states fail to fearlessly oppose federal overreach, the day may rapidly come when the Constitution and individual liberty will be nothing more than remarkable relics of a once-free Republic.

Joe A. Wolverton, II, J.D. is a correspondent for The New American *and travels frequently nationwide speaking on topics of nullification, the NDAA, and the surveillance state. He is the host of The New American Review radio show that is simulcast on YouTube every Monday. Follow him on Twitter*

@TNAJoeWolverton and he can be reached at jwolverton@thenewamerican.com