



The “Secret” PATRIOT Act

Secret PATRIOT Act? What was Wyden talking about?

The American people aren't allowed to know. But they got a taste of how it could be used to suppress freedom a month later, when the *New York Times* reported on June 16 that former CIA supervisor Glenn L. Carle accused senior Bush administration officials of trolling secret CIA files for negative information about one of its public critics, University of Michigan Professor Juan Cole. Cole is the author of a popular blog that had criticized the Bush administration's Iraq policy. The *Times* reported that David B. Low, the National Intelligence Officer (NIO) for Transnational Threats at the National Intelligence Council, asked Carle in 2005: “What do you think we might know about him, or could find out that could discredit him?” After being rebuffed for making an inappropriate request, Low continued:



“But what might we know about him?... Does he drink? What are his views? Is he married?”

Carle rebuffed the request again, stressing that it was illegal. But the next day, the *New York Times* explained, when Carle was “on his way to a meeting in the C.I.A.’s front office, a secretary asked if he would drop off a folder to be delivered by courier to the White House. Mr. Carle said he opened it and stopped cold. Inside, he recalled, was a memo from Mr. Low about Juan Cole that included a paragraph with ‘inappropriate, derogatory remarks’ about his lifestyle.”

“I couldn't believe this was happening,” Carle told the *Times*. “People were accepting it, like you had to be part of the team.”

Low denied ever making such a request, but other details of Carle's account were confirmed by the *Times*, such as verifying that e-mails on Cole had been sent by an assistant to the Office of the Director of National Intelligence, as Carle had claimed. The CIA also denied that the described use of intelligence to destroy the President's critics ever happened. “We've thoroughly researched our records, and any allegation that the C.I.A. provided private or derogatory information on Professor Cole to anyone is simply wrong,” CIA spokesman George Little told the *Times*.

The target of the CIA dirt-digging, Juan Cole, called the spying “outrageous.” Wired.com's Spencer Ackerman summarized the ludicrousness of the CIA's actions: “Bewilderingly, all Cole did was say mean things about the Bush team on the internet. He wasn't a militant, he wasn't even an activist. He blogged. To devote precious intelligence resources, especially from counterterrorism officials, to silencing him is laughably solipsistic.”

**Nothing to Ignore**

But there's nothing laughable about a naked attack on political critics using secret intelligence. U.S. intelligence agencies currently have the capacity to download everything "from" or "through" the Internet, including private e-mails, web traffic, and telephone records. According to a May 23 *New Yorker* article by Jane Mayer, the NSA has indexed private Internet data in a "Google-style" searchable database for intelligence agencies to use. The Juan Cole incident is the first public case where the office of the President allegedly used U.S. intelligence agencies to gather dirt on its critics in the media or of rival politicians since Richard Nixon's "enemies list" in the 1970s.

Some readers might be inclined to say: "I'm not doing anything wrong, so I'm not worried about government wiretapping." But the real power of surveillance is not just discovering illegal acts. Rather, it's in the ability to blackmail and intimidate both the great masses and political opposition leaders. Warrantless surveillance allows the government to find out anything embarrassing about anyone on the Internet. It allows the government to know — and blackmail — people with embarrassing medical histories (substance abuse, mental illness, incontinence, STDs, etc.), Internet traffic (in pornography, foul language, wasted time at work on Facebook, etc.), people who have made negative or angry remarks about bosses (or colleagues, family members, etc.), poor grades in school, disciplinary measures or negative reviews at work, and an almost limitless list of perfectly legal but embarrassing measures.

Even a citizen without any sin (if such a thing exists), who possesses a perfect health, work, and school record, can be impacted by the wide accessibility for blackmail by government officials with such unfettered access to Americans' private data. Even if the perfect person is immune from blackmail, his elected officials, judges, lawyers, or news persons may not be. That "perfect" man or woman should be able to see that the whole of society could be bullied and blackmailed by a government that sees all of its citizens' personal data. Moreover, even completely innocent actions such as purchasing nail polish remover or hydrogen peroxide at the local pharmacy may put a citizen on a federal terrorist watch list, or no-fly list, according to some reports, because the NSA retains such sales records from bank and credit card records. Since 9/11, U.S. intelligence agencies have been sharing data more than ever before. So the TSA and CIA also have access to NSA data.

"The Congress should revisit the PATRIOT Act in the light of the revelation of what was attempted in my regard, and should repeal the d*** thing," Cole wrote on his blog, *Informed Comment*. "Failing that, the federal judiciary should find it unconstitutional, which it is. But one of the things that worries me is that some of the key political and judicial personnel who might want to move against it may themselves already have been victims of surveillance, entrapment and blackmailing. Just how corrupt has our whole governmental apparatus become, that clear violations of our Constitution are blithely accepted?"

Cole is right. The executive branch could be blackmailing federal legislators right now to prevent repeal of the PATRIOT Act, and the American people would not know about it. "We're getting to a gap between what the public thinks the law says and what the American government secretly thinks the law says," Senator Wyden told *Wired.com*'s Spencer Ackerman May 25 in an interview in Wyden's Senate office. "When you've got that kind of a gap, you're going to have a problem on your hands."

Wiretapping Without Warrants

The gap Wyden is describing is vast; it's the size of the entire Internet. The amount of data that the NSA is pulling from the American people can be culled from budget documents for the multi-billion-dollar



Written by [Thomas R. Eddlem](#) on July 14, 2011

data centers the NSA is building around the world. The NSA is now building multi-billion-dollar data storage facilities in Maryland, Utah, Texas, and even the United Kingdom (where the NSA culls Internet data generated abroad). The 1.5-million-square-foot Utah facility alone, which broke ground in January, will store data in the yottabyte range.

What's a yottabyte? According to Devin Coldewey of CrunchGear.com:

There are a thousand gigabytes in a terabyte, a thousand terabytes in a petabyte, a thousand petabytes in an exabyte, a thousand exabytes in a zettabyte, and a thousand zettabytes in a yottabyte. In other words, a yottabyte is 1,000,000,000,000,000GB. Are you paranoid yet?

By some estimates, a yottabyte is the current size of the entire Internet. And keep in mind, that's just the download capacity of the NSA's data center in Utah. It doesn't count the three other NSA data centers in Maryland or the ones in Texas and the United Kingdom.

Clearly, the NSA is not getting court warrants for seizing and storing all that data, as required by the Fourth Amendment to the U.S. Constitution. And Mayer's *New Yorker* article confirmed that the federal government is engaging in surveillance of Americans that entirely ignores the Constitution's Fourth Amendment. According to the *New Yorker*, Diane Roark, a former staff member on the House Permanent Select Committee on Intelligence, asked NSA Director Michael Hayden what privacy protections the NSA had included in its surveillance for Americans:

She says that he "kept not answering. Finally, he mumbled, and looked down, and said, 'We didn't need them. We had the power.' He didn't even look me in the eye. I was flabbergasted."

Mayer then added: "She asked him directly if the government was getting warrants for domestic surveillance, and he admitted that it was not."

Mayer's article also revealed that whistleblowers about the NSA's open violation of the Fourth Amendment to the U.S. Constitution have been persecuted and prosecuted by federal officials. One such victim of the government coverup of the crime against the U.S. Constitution was whistleblower and former NSA official Thomas Drake. "They had made me into an enemy of the state just by saying I was," former NSA official Thomas Drake told Mayer. Drake was charged with a variety of violations of the Espionage Act of 1917 for informing congressional investigators that such a program existed, charges that could bring 30 years in prison. "Telling the truth to congressional oversight committees is leaking?" Drake asked. Apparently, the NSA considers it a serious crime.

Drake eventually pled guilty to a misdemeanor charge of retaining classified documents at his house. Mayer's article, a must-read for anyone who wants to know about the executive branch's attack on the U.S. Constitution, quoted former NSA crypto-mathematician Bill Binney as saying of his invention of an eavesdropping technology: "I should apologize to the American people. It's violated everyone's rights. It can be used to eavesdrop on the whole world."

"It was my brainchild," Binney told Mayer, though he stressed that his original program included anonymizing features to protect privacy. "They removed the protections, the anonymization process. When you remove that, you can target anyone." When the NSA used a version of his software package to spy on the American people's Internet and phone traffic, "my people were brought in, and they told me, 'Can you believe they're doing this? They're getting billing records on U.S. citizens! They're putting pen registers' — logs of dialed phone numbers — 'on everyone in the country!'" Binney eventually decided to resign from the NSA because he "couldn't be an accessory to subverting the Constitution."



Written by [Thomas R. Eddlem](#) on July 14, 2011

Binney told Mayer he “believes that the agency now stores copies of all e-mails transmitted in America, in case the government wants to retrieve the details later.” Mayer notes, “In the past few years, the N.S.A. has built enormous electronic-storage facilities in Texas and Utah. Binney says that an N.S.A. e-mail database can be searched with ‘dictionary selection,’ in the manner of Google. After 9/11, he says, ‘[NSA Director Michael] Hayden reassured everyone that the N.S.A. didn’t put out dragnets, and that was true. It had no need — it was getting every fish in the sea.’”

Cole explained, “What alarms me most of all in the nakedly illegal deployment of the CIA against an academic for the explicit purpose of destroying his reputation for political purposes is that I know I am a relatively small fish and it seems to me rather likely that I was not the only target of the baleful team at the White House. After the Valerie Plame affair, it seemed clear that there was nothing those people wouldn’t stoop to. You wonder how many critics were effectively ‘destroyed.’ It is sad that a politics of personal destruction was the response by the Bush White House to an attempt of a citizen to reason in public about a matter of great public interest.”

Cole attacked the Bush administration for its attempts to use secret intelligence for political purposes, but the Obama administration could be doing the same thing right now. Certainly, the power is in Obama’s hands to publicly discredit or quietly blackmail his political opposition. Police states throughout history — such as the German Gestapo and the Soviet KGB — have always insisted that putting this surveillance power in the hands of government was necessary for public safety, though neither the KGB nor the Gestapo ever had files on the citizens as extensive as what the NSA possesses today. This surveillance power is precisely what the Founding Fathers sought to prevent by ratifying the Fourth Amendment to the U.S. Constitution, which explicitly requires a warrant signed by a judge based upon “probable cause” and specifying what the warrant will find for any search to be constitutional.

— Photo of Michael Hayden: AP Images



Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



[Subscribe](#)

What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.