## New American

Written by Joe Wolverton, II, J.D. on August 16, 2013



## **Google Claims Right to Rifle Through All Gmail Messages**

"If you care about your email correspondents' privacy don't use Gmail." That's the <u>advice given by Consumer</u> <u>Watchdog's Privacy Project director, John M.</u> <u>Simpson</u>.

On August 12, Simpson's organization released a court document filed by Google in a federal case in Northern California District Court.

In the "<u>Motion to Dismiss</u>" obtained by Consumer Watchdog, Google's attorneys argue:



Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use web-based email today cannot be surprised if their emails are processed by the recipient's [email provider] in the course of delivery. Indeed, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."

The tech giant whose very name has become a verb admits to the court, but tellingly not to its millions of users, that there is nothing private in any electronic communication facilitated by its Gmail service.

Regarding the bizarre sender/assistant analogy employed by the white-stocking law firm hired by Google to protect its interests, John Simpson writes, "Google's brief uses a wrong-headed analogy; sending an email is like giving a letter to the Post Office," said Simpson. "I expect the Post Office to deliver the letter based on the address written on the envelope. I don't expect the mail carrier to open my letter and read it. Similarly when I send an email, I expect it to be delivered to the intended recipient with a Gmail account based on the email address; why would I expect its content will be intercepted by Google and read?"

Although Google's admission may be something of an unexpected revelation to the millions of people who rely on Gmail for their electronic communication, there is precedent for the denial of privacy in the third-party transmission of information.

In the case of <u>Smith v. Maryland</u> (1979), the court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."

The court in that case ruled that if someone is talking to another person by way of a medium provided by a third-party (in the Smith case it was a telephone company), both parties must expect that the "intermediary" will have access to the content of the communication.

Regarding the telephone company — analogous to Google in the present case — the court explained that when a person uses a telephone, he "voluntarily convey[s] numerical information to the telephone company and 'expose[s]' that information to its equipment in the ordinary course of business."

In a more recent case, however, the Supreme Court ruled that Internet and telephone communications are not *a priori* devoid of constitutional protection.

"I for one doubt that people would accept without complaint the warrantless disclosure to the

# **New American**

Written by Joe Wolverton, II, J.D. on August 16, 2013



Government of a list of every Web site they had visited in the last week, or month, or year," Justice Sonia Sotomayor wrote in the <u>U.S. v. Jones</u> opinion handed down in January 2012.

Although the case in which Google admitted that it rifles through users' e-mails deals with a complaint regarding Google ads, in <u>an interview with CNBC in 2009</u>, Google Chairman Eric Schmidt referenced the mandates of the Patriot Act as justification for his company's monitoring of customers' e-mail.

"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place," Schmidt said. "But if you really need that kind of privacy, the reality is that search engines, including Google, do retain this information for some time. And ... we're all subject, in the United States, to the Patriot Act, and it is possible that that information could be made available to the authorities."

Not only could that information be made available, that information is funneled directly to the desktops of federal snoops.

*The New American* has reported about the leaked PowerPoint presentation explaining PRISM — the National Security Agency's (NSA) program monitoring the Internet activity of millions of Americans.

Under PRISM, the NSA and the FBI are "tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio, video, photographs, e-mails, documents, and connection logs that enable analysts to track a person's movements and contacts over time," as reported by the *Washington Post*.

As the investigation proceeds, it is becoming apparent that the level of collusion between the surveillance agency and the country's largest tech companies appears much higher than representatives of those corporations would have customers believe.

As if that unconscionable cooperation wasn't enough, stories in other outlets report that the federal government's corporate partners in the construction of the surveillance state are handing over more private customer data than has been revealed so far.

Take, for example, this information contained in <u>a story published by BusinessWeek online</u>:

Through its open-source Android project, Google has agreed to incorporate code, first developed by the agency [the NSA] in 2011, into future versions of its mobile operating system, which according to market researcher IDC runs on three-quarters of the smartphones shipped globally in the first quarter. NSA officials say their code, known as Security Enhancements for Android, isolates apps to prevent hackers and marketers from gaining access to personal or corporate data stored on a device. Eventually all new phones, tablets, televisions, cars, and other devices that rely on Android will include NSA code, agency spokeswoman Vanee' Vines said in an e-mailed statement.

In a 2011 presentation obtained by Bloomberg Businessweek, Smalley listed among the benefits of the program that it's "normally invisible to users." The program's top goal, according to that presentation: "Improve our understanding of Android security."

Vines wouldn't say whether the agency's work on Android and other software is part of or helps with Prism.

The military-industrial-surveillance-technology complex is massive and the threat it poses to the Fourth Amendment can be neither overstated nor overlooked, if liberty is to be preserved.

The aggregate message of these separate accounts is that the federal government, in cooperation with

# **New American**

#### Written by Joe Wolverton, II, J.D. on August 16, 2013



several of the country's largest corporate entities, treats every American citizen as a suspect.

Moreover, the scope of the surveillance is being expanded to gather every word, every movement, every text, every conversation, every e-mail, and every social media post under the never-blinking eye of the federal domestic spying apparatus.

The hour is now late if this Republic is to remain a land under the rule of law. To that end, it is critical that Americans recognize that the sweeping surveillance dragnet thrown by the NSA, FBI, and other federal agencies is in direct, open, and hostile opposition of the fundamental freedoms protected by the Constitution. The Fourth Amendment to the Constitution clearly states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Despite the black-and-white admissions made by Google attorneys in the brief disclosed by Consumer Watchdog, a Google spokesperson told *Business Insider in an e-mail statement: "*We take our users' privacy and security very seriously; recent reports claiming otherwise are simply untrue. We have built industry-leading security and privacy features into Gmail — and no matter who sends an email to a Gmail user, those protections apply."

It appears that Google has one face for its federal co-conspirators and one for the millions of Americans who send millions of monitored messages through its servers.

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 can be reached at <u>jwolverton@thenewamerican.com</u>.



### 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.