Written by **Joe Wolverton, II, J.D.** on July 18, 2013

Despite Participation in PRISM, Microsoft Warns of Threat to Constitution

"The Constitution is suffering." That was the message sent July 16 by Microsoft general counsel Brad Smith in a letter to U.S. Attorney General Eric Holder.

The purpose of the letter was to ask Holder "to get involved personally in assessing the Constitutional issues raised by Microsoft and other companies that have repeatedly asked to share publicly more complete information about how we handle national security requests for customer information."

The "requests for customer information" referred to by Smith are part of the PRISM program exposed in the cache of National Security Agency (NSA) documents leaked by whistleblower and former NSA contractor Edward Snowden.

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*.

Microsoft's sudden concern for the health of the Constitution is curious given the substantial evidence of their covert collusion in the PRISM program.

Consider, for example, the information published by the *Guardian* (U.K.) on July 12:

> Microsoft has collaborated closely with US intelligence services to allow users' communications to be intercepted, including helping the National Security Agency to circumvent the company's own encryption, according to top-secret documents obtained by the *Guardian*.

Following that claim, the paper then enumerates specific examples of Microsoft's disregard for the very principles of liberty they purport to hold as "first and foremost" and that they seek protection of from Eric Holder. Here are some of the *Guardian's* revelations:

> The documents show that:
>
> • Microsoft helped the NSA to circumvent its encryption to address concerns that the agency would be unable to intercept web chats on the new Outlook.com portal;
>
> • The agency already had pre-encryption stage access to email on Outlook.com, including Hotmail;
>
> • The company worked with the FBI this year to allow the NSA easier access via Prism to its cloud storage service SkyDrive, which now has more than 250 million users worldwide;
>
> • Microsoft also worked with the FBI's Data Intercept Unit to "understand" potential issues with a feature in Outlook.com that allows users to create email aliases;
>
> • In July last year, nine months after Microsoft bought Skype, the NSA boasted that a new

capability had tripled the amount of Skype video calls being collected through Prism;

• Material collected through Prism is routinely shared with the FBI and CIA, with one NSA document describing the program as a "team sport".

In their own defense, the Microsoft missive to Holder insists that these disclosures have been "misinterpreted" in the media.

Then, Microsoft practically pleads with the Obama administration to allow it to publicly rend its garments and sit in sackcloth and ashes, demonstrating the sincerity of its repentance.

Should anyone disbelieve the length to which Microsoft is willing to go to deflect deeper inquiry by customers and journalists into the quantity and quality of personal information the Redmond, Washington, tech giant gave to federal snoops, consider the cloying tone in the following excerpt from the letter:

> As I know you appreciate, the Constitution guarantees the fundamental freedom to engage in free expression unless silence is required by a narrowly tailored, compelling Government interest. It's time to face some obvious facts. Numerous documents are now in the public domain. As a result, there is no longer a compelling Government interest in stopping those of us with knowledge from sharing more information, especially when this information is likely to help allay public concerns.
>
> I feel very fortunate that we have both an Attorney General and a President with such longstanding knowledge of and appreciation for our Constitution. Put simply, we need you to step in to ensure that common sense and our Constitutional safeguards prevail.

The way, then, that Microsoft's general counsel suggests for shoring up "Constitutional safeguards" is to go along for years with the government's secret surveillance of its customers, then, when the heat is on, claim "the devil made me do it" and write letters lamenting their participation in the snooping and touting their love for liberty.

Then, to multiply the manifold embarrassments of its narrative, Microsoft betrays its sycophancy by praising the president's commitment to the Constitution. This needs no elaboration in order to further prove the point.

In another section of the letter to Holder, Microsoft accuses the government of keeping the company from "making adequate progress" in its goal of complete disclosure of its dealing with the NSA. Then Microsoft hedges, applauding the "good faith in which the Government has dealt with us during this challenging period."

One aspect of the purported "good faith" Microsoft (and many of its corporate colleagues) point to is the oversight of the FISA court, the secret court which rules on the legality of the federal government's petitions for wiretapping warrants and other surveillance requests. The problem is that while in theory it functions as a check on unconstitutional surveillance, in reality the FISA court is its champion.

Documents obtained by the *Guardian* reveal that the court routinely grants the NSA and others the go-ahead to use data "inadvertently" collected during unwarranted surveillance of American citizens.

The newspaper that broke the story of the NSA's activities as revealed by whistleblower Edward Snowden published on June 20 "two full documents submitted to the secret Foreign Intelligence Surveillance Court." Both documents were signed by Attorney General Eric Holder and were issued in July 2009.

According to the article written by Glenn Greenwald and James Ball, the documents "detail the procedures the NSA is required to follow to target 'non-US persons' under its foreign intelligence powers and what the agency does to minimize data collected on US citizens and residents in the course of that surveillance."

Not surprisingly, neither the Fourth Amendment nor the freedoms against tyranny that it protects are honored by Holder or the other architects and construction crews erecting the surveillance state.

As Greenwald and Ball report, the leaked documents demonstrate that when the NSA is conducting surveillance under the pretense of monitoring foreign targets, any U.S. communication caught in the dragnet is "collected, retained and used."

Using Section 215 of the Patriot Act as justification, the NSA is now known to monitor and seize the phone records of millions of Americans who are not now or never have been suspected of any crime that would justify the issuing of a search warrant. This wholesale watching of the telephone activities of citizens was revealed by the *Guardian* a few weeks ago as part of Snowden's release of information on his former employer.

With regard to the lack of oversight provided by the so-called FISA court, *The New American* reported in May that, as required by provisions of the Foreign Intelligence Surveillance Act Amendments of 2008 (FISA) and the Patriot Act (as amended in 2005), the Department of Justice revealed to Congress the number of applications for eavesdropping received and rejected by the FISA court.

The letter addressed to Senator Harry Reid (D-Nev.) reports that in 2012, of the 1,789 requests made by the government to monitor the electronic communications of citizens, not a single one was rejected.

That's right. The court, established specifically to judge the merits of applications by the government to spy on citizens, gave a green light to every government request for surveillance.

All these activities violate the Fourth Amendment requirement that "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." In practical terms, that means that the federal government cannot purposely monitor the phone or Internet communications carried on by an American or a person inside the United States without a qualifying warrant.

Of course, by tapping directly into the servers of the world's most popular purveyors of Internet services — with the cooperation of those companies — the federal government bypasses all legal and constitutional restraints on its already immense power.

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 jwolverton@thenewamerican.com*