Written by Joe Wolverton, II, J.D. on July 7, 2013

Tech Companies Hiding Depth of Cooperation with NSA Surveillance

The New American and others continue to comb through 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 spying apparatus' corporate partners in the construction of the surveillance state are handing over more private customer data than has been revealed so far.

For example, consider this story published by Bloomberg:

> Thousands of technology, finance and manufacturing companies are working closely with U.S. national security agencies, providing sensitive information and in return receiving benefits that include access to classified intelligence, four people familiar with the process said.
>
> In addition to private communications, information about equipment specifications and data needed for the Internet to work — much of which isn't subject to oversight because it doesn't involve private communications — is valuable to intelligence, U.S. law-enforcement officials and the military.
>
> Microsoft Corp., the world's largest software company, provides intelligence agencies with information about bugs in its popular software before it publicly releases a fix, according to two people familiar with the process.
>
> Larry Page, chief executive officer of Google Inc., said in a blog posting June 7 that he hadn't heard of a program called Prism until after Edward Snowden's disclosures and that the company didn't allow the U.S. government direct access to its servers or some back-door to its data centers.
>
> These programs, whose participants are known as trusted partners, extend far beyond what was revealed by Edward Snowden, a computer technician who did work for the National Security Agency. The role of private companies has come under intense scrutiny since his disclosure this month [June] that the NSA is collecting millions of U.S. residents' telephone records and the

> computer communications of foreigners from Google Inc (GOOG). and other Internet companies under court order.
>
> Many of these same Internet and telecommunications companies voluntarily provide U.S. intelligence organizations with additional data, such as equipment specifications, that don't involve private communications of their customers, the four people said.

And this, from Reuters:

> Former U.S. officials and intelligence sources say the collaboration between the tech industry and spy agencies is both broader and deeper than most people realize, dating back to the formative years of Silicon Valley itself.
>
> As U.S. intelligence agencies accelerate efforts to acquire new technology and fund research on cybersecurity, they have invested in start-up companies, encouraged firms to put more military and intelligence veterans on company boards, and nurtured a broad network of personal relationships with top technology executives.
>
> And they are using those connections to carry out specific espionage missions, current and former officials say, even as they work with the tech industry to avoid overt cooperation that might raise the hackles of foreign customers.
>
> Joel Harding, an intelligence officer for the Joint Chiefs of Staff in the 1990s who went on to work at big defense contractors Computer Sciences Corp and SAIC, said spy agencies have at times persuaded companies to alter their hardware and software products to enable monitoring of foreign targets.

This last disturbing disclosure corresponds in many material ways to a story published by BusinessWeek online:

> 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.

How does the NSA come by such root-level access to technology millions of Americans rely on every day for hundreds of reasons?

Again, from Reuters:

> Despite these secret collaborations, former intelligence officials and company executives say the great fear of overseas customers — that widely used U.S. technology products contain a "back door" accessible only to the National Security Agency or Central Intelligence Agency — is

> exaggerated. They said computers and communications overseas are captured by other means, including third parties such as the laptop reseller and special software developed by the agencies.
>
> Defense contractors offer the government the means to break in to the products of virtually every major software vendor, according to a product catalogue reviewed by Reuters that was described as typical for the industry.

The scope of the surveillance and the collusion appears to be much more widespread and incestuous than previously reported.

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 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 deprivation 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.

In the wake of the presentation of this appalling evidence of government-corporate collusion in the constant surveillance of innocent citizens, have Americans rushed to rid themselves of the devices sold to them by Silicon Valley?

No. According to BNAMericas online:

> Worldwide smartphone sales are expected to reach 1bn units in 2013, compared to 675mn in 2012, research and consultancy firm Gartner said in a release.
>
> Meanwhile, tablets are also expected to see continued rapid growth this year, with unit sales increasing 69.8% to 197mn.

The decline of liberty, it seems, has done nothing to slow the growth of dependence on the very tools being used to build the surveillance state.

Photo: AP Images

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*