blog.ted.com /reading-on-the-state-of-digital-privacy-nsa-surveillance/

# Further reading on NSA surveillance and the state of digital privacy

Posted by: Kate Torgovnick May November 7, 2013 at 1:47 pm EST ⋮ 10-13 minutes

Technology TED Talks

## The internet, the perfect tool for the surveillance state? Further reading (and watching) on the state of digital privacy

Mikko Hypponen speaks just last week at TEDxBrussels, expressing outrage at the NSA.

“We already knew this.” “It’s necessary for the War on Terror.” “Other countries are doing it too.” “But I have nothing to hide.” These are the most common reasons people express for not feeling outrage over the revelations this year that the United States’ National Security Agency has been involved in widespread surveillance. Mikko Hypponen: How the NSA betrayed the world's trust -- time to act In today’s blistering talk, security expert Mikko Hypponen shares why he is hopping mad about the NSA’s actions, and why every user of the internet should be equally enraged. Because at the end of the day, he says, these rationalizations obscure a shocking fact: because the world relies on American companies for its information needs, virtually every user of the internet is being watched.

Digital privacy is, obviously, something on many of our minds. Below, a collection of articles, think pieces, op-eds and TED Talks on the state of digital privacy, some that echo Hypponen’s vigor and some that offer differing opinions.

**1. The story that started it all**. In June, when journalist Glenn Greenwald first broke the story in *The Guardian* that the NSA was collecting Verizon phone records for millions daily, and that the Prism program was tapping into the data of major tech companies, some were riveted and outraged while some tuned out because the news at first glance didn’t sound shocking. So, in case you missed them, read the initial stories that would eventually make Edward Snowden a household name. While Greenwald just announced that he is leaving *The Guardian* after 14 months of reporting this story, for now, his column “On Security and liberty” is a great resource for the latest revelations in just how far this surveillance goes. The most recent articles: “NSA and GCHQ target Tor network that protects anonymity of web users” and “NSA shares raw intelligence including Americans’ data with Israel.”

**2. The deep look at the data**. *The New York Times* and *The Guardian* have just completed a pair of in-depth analyses of the documents they received from Snowden in June. Both concluded that no information, no matter how small or seemingly irrelevant, escaped the NSA’s purview. *The New York Times* described the NSA’s strategic plan as that of an “electronic omnivore… eavesdropping and hacking its way around the world to strip governments and other targets of their secrets.” According to the leaked documents, only 35% of the NSA’s efforts are focused on collecting information on terrorist activities. The NSA is spying on both friends and foes, using information to gain “diplomatic advantage” over US allies like France and Germany, and “economic advantage” over growing economies like Japan and Brazil.

**3. A new revelation this week: evidence that the NSA and (its British counterpart) GCHQ hacked Google and Yahoo**. In his talk, Hypponen points out how strange it is that, while leaked documents show the exact dates that the NSA began monitoring major American providers, many of these providers had also stated publically that they hadn’t given backdoor access. Just days after Hypponen’s talk was delivered, new evidence emerged that Google and Yahoo had indeed been hacked — not by tapping into the software, but by tapping into their private networks via leased fiber. This *Washington Post* article gives a nice explanation of how we know that the NSA had access to internal cloud data from these companies. And read Google’s hopping mad response to this news, which they call “industrial scale subversion.” A member of the TED tech team points out that this doesn’t necessarily support the solution Hypponen shares in his talk — to create alternatives to American providers. “This was not happening just within the US, but on international soil as well,” he explains.

**4. A valid question: who is watching the watchers?** In late October, another new wrinkle in this story emerged, which Hypponen mentions in his talk — that the NSA was monitoring the telephones and emails of 35 world leaders, including Angela Merkel of Germany, Dilma Rousseff of Brazil and Felipe Calderón of Mexico. And apparently, President Barack Obama did not sign off on this … or even know about it until an internal review in the wake of the NSA revelations this summer. Here, the *Washington Post* breaks that story, while John Cassidy of the New Yorker thinks more deeply about what it means, writing, “From the very beginning of this, the biggest question has been about the supervision—or lack of supervision—of the spying agencies: Who watches the watchers?”

[youtube=http://www.youtube.com/watch?v=h0d_QDgl3gI&w=586&h=440]

**5. Another interpretation of NSA outrage: a battle for power on the internet**. In this talk from TEDxCambridge, security expert Bruce Schneier (the man who pointed out “The security mirage”) gives a fascinating analysis of why revelations of NSA, GCHQ and other government surveillance programs are so shocking — because they represent a shift. For the first part of the internet’s history, the medium gave power to those traditionally without it — to individuals and grassroots organizers. But now, the internet is increasingly becoming a tool for traditional powers like governments and international corporations. So where does this leave the majority of citizens? Stuck in the middle, says Schneier. (Bonus: Read both Schneier and Hypponen’s initial take on the revelations of NSA surveillance, given to the TED Blog this summer.)

**6. An alternative cloud service**. In his talk, Hypponen ends with a call for people outside of the United States to band together to create Open Source, secure alternatives to American internet companies. And Hypponen’s company, F-Secure, has just launched one such alternative: Younited, a personal cloud service hosted in Finland, which has strict privacy laws. Hypponen writes of the service, “It’s high time for a fresh European alternative to enter the market, taking the existing Internet behemoths head on. What the world needs now is a cloud storage service that is not subject to uncontrolled access by intelligence agencies.”

**7. But is Open Source the answer?** TED’s tech team is not convinced. “I’d rather trust an open source project than a closed one any day of the week. But Open Source is not a silver bullet,” says one team member. “You can see even back in 2003 people tried to back door the Linux kernel. This patch was submitted in a strange way so it was caught but the code looks so innocent that if it was part of a normal merge it might not have been caught. Those three lines of code would give anyone root access — god access on linux systems. As of 2012, there are over 15 million lines of code.” Just for fun, he suggests watching this YouTube clip of what happened recently when the creator of the Linux kernel was asked if he has been approached by the NSA about giving backdoor access, as it will definitely scare you. And another team member agrees: “The solution is not so much Open Source and governments, but probably strengthening the whitehat community around Open Source.”

**8. Another rebuttal to Hypponen: why we can’t cut off the data flow between the U.S. and the world**. Cameron Kerry, the General Counsel of the US Department of Commerce, recently gave a speech warning against a solution like the one Hypponen forwards. According to the blog The Hill, Kerry argues that cutting off the flow of data between Europe and the United States would be a mistake. “It would cause significant and immediate economic damage,” he says. “Moreover, it would lead to loss of competitiveness on both sides, as other economies around the world that embrace open Internet architectures and freedom to experiment with data analytics offer havens for innovators … Our economic future is at stake in our international engagement.” (Note: Kerry will speak soon at TEDxBeaconStreet.)

**9. The end of the internet?** Security experts are echoing Kerry’s concerns: according to *The Guardian*, they are now warning that this data collection policy might lead to the dissolution of the Internet as we know it. Countries like Brazil, Germany and India have begun encouraging regional online users to route their data locally rather than over the monitored US and UK servers. Indian government employees, for example, have been advised not to use the US-based Gmail, and to type up sensitive documents on typewriters, rather than on a computer. For a system that is based on interconnectivity, the implications of a fractured and localized Internet pose a threat to the network, global economies, and our access to information.

**9. In defense of the program**. Meanwhile, U.S. officials are standing firmly in support of the NSA surveillance program, insisting that it is effective and necessary. General Keith B. Alexander, director of the NSA, said last month that he saw no effective alternative to the government's program of collecting electronic metadata in the fight to prevent terrorism. Senator Dianne Feinstein, chairman of the Senate Intelligence Committee, published an op-ed in *USA Today* strongly defending the program, arguing that the program has been effective in helping to prevent terrorist plots against the U.S. and its allies. And, for the first time, information collected by the NSA is being used to build a criminal case around a suspected terrorist. Jamshid Muhtorov, who is accused of supporting the Islamic Jihad Union, was informed that data collected in his private communications was used to arrest him. This case is expected to precipitate further legal action and possibly head to the Supreme Court.

[ted id=1848]

**11. Other major threats to privacy: facial recognition, social media, and cell phone GPS**. In his recent TED Talk, "Why privacy matters," behavioral economist Alessandro Acquisti sounded a warning bell on the fact that facial recognition abilities are exponentially improving while, meanwhile, the line between personal and public is blurring via social networking sites. In his talk, he warns that we are about to have an Adam and Eve moment — where all of a sudden, we realize we aren't wearing any clothes. "Any personal information can become sensitive information," he says. (Read the TED Blog story: The future of facial recognition.) In another chilling TED Talk, "Your cell phone company is watching," German politician Malte Spitz shares what happened when he asked his cell phone company to share the data they were collecting on him. The result: 35,830 lines of code that added up to a nearly minute-by-minute account of half a year of his life.

*Liz Jacobs contributed heavily to this article.*

Previous Chapter Next Chapter