One Year Later: Electronic Frontier Foundation Takes A look At The Edward Snowden Leaks And How Government Spying Affects Us All

Posted on May 16, 2014 by Electronic Frontier Foundation
32 Shares

This essay, written by EFF International Rights Director Katitza Rodriguez, was originally published on the foundation's website May 15.

June 5th marks the first anniversary of the beginning of the Edward Snowden revelations–a landmark event in global awareness of the worldwide spying machine. It has been a year where the world has learned that the NSA and its four closest allies in the Five Eyes partnership (United Kingdom, Canada, Australia, and New Zealand) have been spying on much of the world's digital communications. What have we learned?

The foreign intelligence agencies of these nations have constructed a web of interoperability at the technical and operational levels that spans the entire globe. We have learned the extent of the cooperation and intelligence sharing amongst these countries, and have witnessed how material gathered under one country's surveillance regime is readily shared with the others. The strategic location of the Five Eyes countries enables them to surveil most of the world's Internet traffic as it transits through their hubs and is stored in their various territories. Moreover, they have partnered with over 80 major global corporations to leverage their spying capabilities. The scope and reach of their cooperation and intelligence sharing has shocked the world, including many who were previously unaware of the privacy threats that EFF has been covering since 2005.

In a leaked internal document, the NSA defined their "posture" as, "Sniff, know, collect, process, exploit, partner it all." This last year, we have learned that the NSA has strayed far from its legitimate goal of protecting national security. In fact, we have seen the NSA participate in economic espionage, diplomatic spying and suspicionless surveillance of entire populations. Even worse, the NSA has also surreptitiously weakened the products and standards that Internet users use to protect themselves against online spying.

In his new book about working with Snowden, *No Place To Hide*, journalist Glenn Greenwald lays out some alarming facts that have been revealed in the year of leaks:

- In a 30 day period, the NSA collected almost 3 billion telephone calls and emails that had passed directly through US telecom networks. As Greenwald explained, that exceeds the collection of each of the systems from "Russia, Mexico, and virtually all countries in Europe, and roughly equal to the collection of data from China."
- In a 30 day period, a single NSA unit had collected data on more than 97 billion emails and 124 billion phone calls from around the world.
- In a single 30 day period, the NSA has collected 500 million pieces of data from Germany, 2.3 billion from Brazil, and 13.5 billion from India.
- The NSA has collected 70 million pieces of metadata in cooperation with France, 60 million with Spain, 47 million with Italy, 1.8 million with the Netherlands, 33 million with Norway, and 23 million with Denmark.

In addition, the Snowden report has brought to light a three-tiered hierarchy of NSA partnerships with foreign governments. As reported by Greenwald's book:

TIER 1: Five Eyes is an agreement between the U.S. and United Kingdom, Canada, Australia, and New Zealand to collaborate on global spying while voluntarily restricting their own spying on one another unless specifically requested to do so by a partner country's own officials.

TIER 2: Countries that the NSA works with for specific surveillance projects while also spying heavily on them. These include mostly European countries, some Asian countries, and no Latin American ones.

TIER 3: Countries on which the United States routinely spies but with whom it virtually never cooperates: Brazil, Mexico, Argentina, Indonesia, South Africa, Kenya are some democratic countries that are on the list.

Finally, we now know of the following covert NSA operations:

EGOTISTICAL GIRAFFE: The NSA has targeted the Tor browser, an anonymity tool enabling Internet users to browse the net anonymously.

MUSCULAR: Launched in 2009, MUSCULAR infiltrates links between global data centers of technology companies such as Google and Yahoo not on U.S. soil. These two companies have responded to MUSCULAR by encrypting these exchanges.

XKEYSCORE: The software interface through which NSA analysts search vast databases collected under various other operations. XKEYSCORE analyzes emails, online chats and the browsing histories of millions of individuals anywhere in the world. The XKEYSCORE data has been shared with other secret services including Australia's Defence Signals Directorate and New Zealand's Government Communications Security Bureau.

BULLRUN: Not in and of itself a surveillance program, BULLRUN is an operation by which the NSA undermines the security tools relied upon by users, targets, and non-targets. BULLRUN represents an apparently unprecedented effort to attack security tools in general use.

DISHFIRE: The Dishfire operation is the worldwide mass collection of text messages and other phone records, including location data, contact retrievals, credit card details, missed call alerts, roaming alerts (which indicate border crossings), electronic business cards, credit card payment notifications, travel itinerary alerts, meeting information, etc. Communications from U.S. phones have been allegedly minimized, although not necessarily purged, from this database. The messages and associated data from non-U.S.-persons were retained and analyzed.

CO-TRAVELER: Under this operation, the U.S. collects location information from global cell towers, Wi-Fi, and GPS hubs. This information is collected and analyzed over time, in part in order to determine a target's traveling companions.

OLYMPIA: Canada's program to spy on the Brazilian Ministry of Mines and Energy.

BLARNEY: A program to leverage unique key corporate partnerships to gain access to high-capacity international fiber optic cables, switches and routers throughout the world. Countries targeted by Blarney include: Brazil, France, Germany, Greece, Israel, Italy, Japan, Mexico, South Korea, and Venezuela as well as the European Union and the United Nations.

and much more ….

While the Snowden revelations have proved invaluable in confirming the existence of global, cross-border spying by the NSA (and its four primary allies), the governments of the affected billions of Internet and telephone users have been slow to fight back. In some cases, America's allies might be holding back because of their own tangled complicity in this shared network – or else, like Russia and China, they have their own pervasive surveillance networks and arrangements to protect.

But now that a year has passed it's clear that we need to update both our global technical infrastructure and local laws, consistent with long-standing international human rights standards, in order to regain any reasonable degree of privacy. Specifically, we must end mass surveillance. Politicians in every country need to stand up to the NSA's incursions on their territory; the United States needs to reform its laws to recognize the privacy rights of innocent foreigners, and the international community needs to set clear standards which makes any state conducting mass surveillance a pariah.

This entry was posted in Liberty News, Privacy, Staff Reports. Bookmark the permalink.

Post navigation

← Friday Morning News Roundup 5-16-2014
Republican Establishment Faces Test In Tuesday's Primaries →

Electronic Frontier Foundation

From the Internet to the iPod, technologies are transforming our society and empowering us as speakers, citizens, creators, and consumers. When our freedoms in the networked world come under attack, the Electronic Frontier Foundation (EFF) is the first line of defense. EFF broke new ground when it was founded in 1990—well before the Internet was on most people's radar—and continues to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today. From the beginning, EFF has championed the public interest in every critical battle affecting digital rights.
https://www.eff.org/