Your on the Street Reporter

Uyless Black

A Coin Toss on Who Reads our Mail

A Coin Toss on Who Reads Our Mail

May 25, 2014 and September 20, 2014

Hello from Your on the Street Reporter. This report continues the series on the subject of privacy and security in the Internet. I have been waiting to see the President's reaction to the findings and recommendations of the Review Group on Intelligence and Communications Technologies (released December 12, 2013). This group was created by President Obama. Report XIII of this series provides an overview of its conclusions (posted April 6, 2014 at Blog.UylessBlack.com).

According to a White House press release:

> The President noted that the group's report represented a consensus view, particularly significant given the broad scope of the members' expertise in counterterrorism, intelligence, oversight, privacy and civil liberties. The President again stated his expectation that, in light of new technologies, the United States use its intelligence collection capabilities in a way that optimally protects our national security while supporting our foreign policy, respecting privacy and civil liberties, maintaining the public trust, and reducing the risk of unauthorized disclosure. The President expressed his personal appreciation to the group members for the extraordinary work that went into producing this comprehensive and high quality report, and outlined for the group how he intends to utilize their work.[1]

No other words from the White House on the matter. So, we must wait to see what happens at the executive level. I will keep you informed as events unfold.

To the gist of this report: Toss a coin. Heads, Google and other Internet vendors read your email and voice calls. Tails, Uncle Sam does. But then, forget the coin toss, as your electronic correspondence is being read by both private industry and the government. Here is a paraphrased statement from Wikipedia:

> PRISM is an electronic surveillance program launched in 2007 by the National Security Agency (NSA). The PRISM program collects stored Internet communications based on demands made to Internet companies such as Google. Under Section 702 of the FISA Amendments Act of 2008, organizations must turn over any data that match court-approved search terms. The NSA can use these requests to target communications that were encrypted when they traveled across the Internet backbone, to focus on stored data that telecommunication filtering systems discarded earlier.[2]

Figure 2 shows the dates that the government established for companies to make their files available. Some companies protested, but to no avail.[3] For example, Yahoo was threatened with a fine of $250,000 a day for non-compliance. Yahoo lost its appeal in a court ruling:

[1] [1] http://www.whitehouse.gov/the-press-office/2013/12/18/president-obama-s-meeting-review-group-intelligence-and-communications-t

[2] Key-in PRISM.

[3] http://www.wired.com/2014/09/feds-yahoo-fine-prism/

Yahoo fought back on Fourth Amendment grounds, insisting that such a request required a probable-cause warrant and that the surveillance request was too broad and unreasonable and, therefore, violated the Constitution.

Yahoo also felt that warrantless requests placed discretion for data collection "entirely in the hands of the Executive Branch without prior judicial involvement" thereby ceding to the government "overly broad power that invites abuse" and possible errors that would result in scooping up data of U.S. citizens as well.

The request for data initially came under the Protect America Act, legislation passed in the wake of the 9/11 terrorist attacks that allowed the Director of National Intelligence and the Attorney General to authorize "the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States" for periods of up to one year, if the acquisition met five criteria. The Protect America Act sunset in February 2008, but was incorporated into the FISA Amendments Act in July that year.[4]

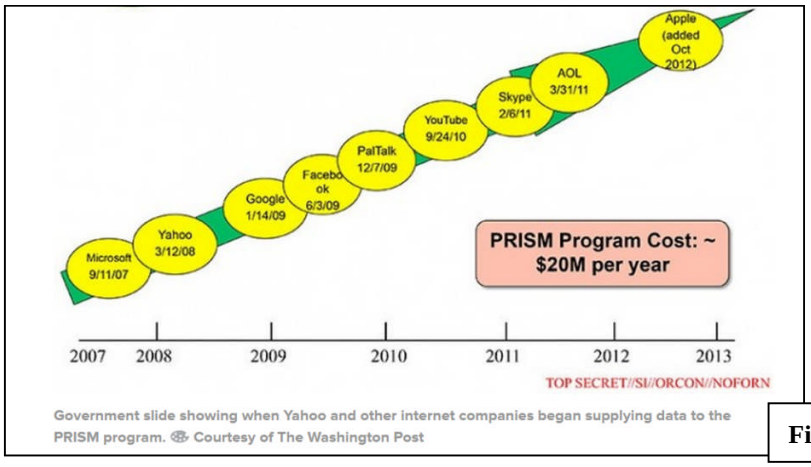

Figure 2. PRISM's subjects.

The present practice, one in which Microsoft, Yahoo, Google, Uncle Sam and others (see Figure 3) routinely examine what should be private emails and telephone conversations, will only grow.[5] Our generation that is presently on earth will continue to have privacy through the postal service, but our future relatives will not. It is only a matter of time when conventional mail---hard copy letters---will cease to exist.

[4] Ibid.
[5] This figure is sourced from Front Line's May 20, 2014 program, via PBS.

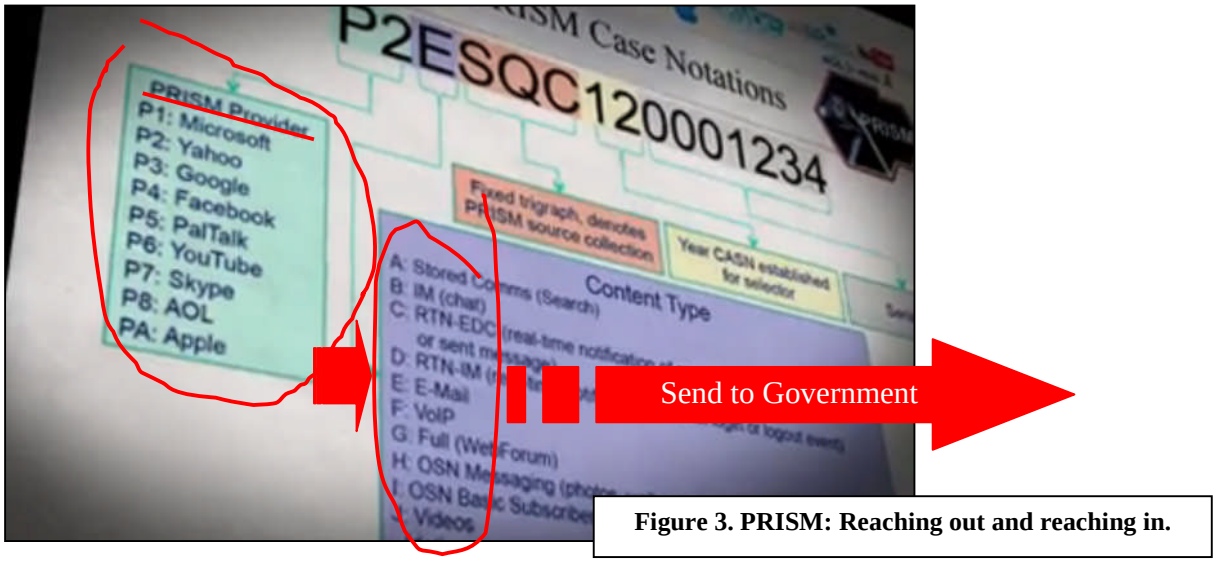

Figure 3. PRISM: Reaching out and reaching in.

As stated several times in this series, I support my government spying on me, but not in the way it has been described in this series. Further, I do not support Google or any other commercial company reading my mail, *especially to sell me something*.

To the issue of government spying, a respected, knowledgeable member of The Review Group on Intelligence and Communications Technologies, Richard Clarke, offered this (paraphrased) thought: *We better be sure that what we create for the present is not used against us in the future.*

But how do we do that? We are not all that clairvoyant or prescient to begin with. I offer three ideas. (1) We go through the admittedly cumbersome process of doing the spying within the confines of the Constitution (which our government did not do). (2) We have sunset clauses on these operations, subject to Congressional and court reviews. (3) We ask the intelligence community: If your programs are so successful, why not let both terrorists and non-terrorists know? You do not have to divulge your methods, only your results. This semi-transparency would allow the citizen to participate in this vital process, without compromising your programs. And who knows? Perhaps it will discourage the terrorist.

It is not the spying that upsets Americans. It is the illegal spying. It is also the lack of accountability on the effectiveness of the spying. Americans may be spending tons of money on worthless programs. But we do not know. Even worse, we have come to learn that Uncle Sam can know a lot about us, but we cannot know much about Uncle Sam. That is no way to run a democracy.

