**Your on the Street Reporter**

**Uyless Black**

# Who Are the Watchdogs Watching?

# Who are the Watch Dogs Watching?

**Summer of 2014**

Recently, several newspapers published reports that the National Security Agency (NSA) has the ability to read our heretofore secure (encrypted) Internet traffic. Examples are emails, bank statements, IRS audits, court summons, and medical letters from doctors.[1]

The articles claim NSA, and its British counterpart, Government Communications Headquarters (GCHQQ), are now able to break the encryption codes that are used by companies such as Microsoft and Google to protect the privacy of our electronic correspondence.

I am not convinced these organizations have developed this capability. The news on this subject stopped almost as soon as it started. It might have been reported in error. My guess is that the advanced encryption systems have not been broken. But users are often careless, and snoopers might be able to by-pass certain measures users employ, or more seriously, do not bother to employ. Before posting the next report to this series, I will do some more snooping myself and get back to you. For now, there is plenty on the table to keep us occupied.

**Security vs. Privacy**

Several years ago**,** I came across this quote while walking through the Spy Museum in Washington, D.C.: "Simply put, it is possible to have convenience, if you do not want security. But if you want security, you must be prepared for inconvenience." (General Benjamin W. Chidlaw, December 1954)

The issue is not just one of convenience or inconvenience. General Chidlaw is correct, but he scratches the surface. Paraphrasing his quote: It is possible to have privacy if you do not want security. But if you want security, you must be prepared to have less privacy. The question is how much security do we need in relation to how much privacy we relinquish?

Should this question be answered by the citizenry of America? After all, it is the citizens who are under scrutiny. But NSA and others in government have made that decision for us. Their rationale is: *Ordinary beings cannot be allowed to know the extent that information on their personal lives is being captured in data bases. To do so would expose the interworkings of what must remain secret. If they are exposed to this information, the terrorists will also learn about it. The revelation will aid the terrorists' efforts to avoid being detected.* Thus, ordinary citizens can never know what Uncle Sam is learning about them.

**Big Data and Big Processors**

In press releases and a congressional paper that I will discuss later in this series, the United States government has informed its citizens what it is collecting on them. But the government is not informing anyone what it is *inferring* from the data it collects. This leads to the idea of *Big Data*.

Big Data is built on the premise that through the massive use of massive computers on massive amounts of data, profiles of behavior can be detected. Big Data theorists even postulate that eventually the Big Data's very smart software operating on many computers (working in parallel with one another) will be able to construct personality profiles capable of predicting

[1] For this report, I will assume the ability exists, because that is the claim of recent news releases. I hesitate, as it is not known how extensive this ability is. There are different kinds and levels of security systems. The documents released by Snowden do not describe the specific encryption/decryption technologies.

 

specific actions. This capability already exists in certain conditions and circumstances. It has been demonstrated in several research projects. Big Data does big profiling.

What if the profiles are wrong? What if the predictions are in error? What if the data that feeds these models are not correct? As software programmers have long observed, the software may be impeccable, but the data may not be worth much: Garbage in, garbage out. Citizens will never know. Because if they are allowed to know, so will the terrorists. Thus, the government officials have a fail-safe reason for keeping citizens in the dark: Any transparency of their snooping would give away their procedures for keeping the terrorists at bay.

**Reality and Virtual Watchdogs**

Let me be clear. From previous reports, I have stated I understand the reasons behind the United States government being permitted to read my mail. The world is populated with people whose sole mission is to do America in. They have no other agenda. I am thankful the NSA exists.

Let me be equally clear about another related matter. During the past few days, it has become evident that the NSA (and who knows about the CIA, DIA, and FBI) has initiated extensive spying without the knowledge of people who are supposed to be America's watch dogs on this kind of behavior. These watch dogs are legally obligated to guard citizens' privacy by monitoring the NSA to make certain NSA is performing its operations in accordance with laws. It appears ordinary citizens have no one in their corner. Citizens' final-stop watchdog, the people elected to Congress, claim they were not aware of the NSA snoopings.

In certain instances, and operating beyond congressional mandates, NSA has assumed the mantle of authority for deciding what to do with citizens' information. NSA claims otherwise, but I will furnish documentation (legally obtained from public media, government paper, and court rulings) that counter NSA's claims.

Obama did not know the NSA was tapping Angela Merkel's email and phone calls. Paul Pillar, an intelligence expert, says the president cannot and should not go down to this level of detail. I cannot disagree strongly enough. It is one thing to delegate the decision of spying on Uyless Black and be done with it. Although Uyless Black would not like it, my resentment would not have major consequences on America's businesses and relationships with…well, the world. It is a different matter to be unaware of the programs of an intelligence agency that have major implications on America's international diplomacy. It is unfathomable that a spy agency decides on its own that it will spy on the head of state of an ally.

Senator Dianne Feinstein chairs the Senate Intelligence Committee. This committee has the responsibility for monitoring NSA and other intelligence agencies. Yet Senator Feinstein was not aware that NSA was reading Ms. Merkel's email. The senator said:

> With respect to NSA collection of intelligence on leaders of U.S. allies---including France, Spain, Mexico and Germany---let me state unequivocally: I am totally opposed. Unless the United States is engaged in hostilities against a country or there is an emergency need for this type of surveillance, I do not believe the United States should be collecting phone calls or emails of friendly presidents and prime ministers.[2]

[2] Jim Michaels and Aaamer Madhani, "Uproar Could Spark Changes to Spying not Seen Since the 1970s," USA TODAY, October 31, 2013.

If the chair of the Senate Intelligence Committee was unaware of this activity, then who in government authorized it? As of this writing, it appears to have been the NSA itself. But not everyone is concerned. Aki Peitz, a former U.S. government counterterrorism official, said:

> …What is there to reform? The U.S. intelligence service is the most overseen intelligence service in the world. There is a lot of oversight. The intelligence committees have access to everything.[3]

**Should Uncle Eavesdrop?**

I reluctantly support the U.S. government's eavesdropping on its citizens, if it is done *discriminately, if it is executed through a court order, if it is not scooping up everything, and if it has a sundown clause for its snooping operations to expire.* But for such a high profile case as eavesdropping on Ms. Merkel, I am not convinced the information gained is worth its costs. As one example among many, how can, say, Brazil permit Google to store information about Brazil's citizens if the United States government has access to that data? That's the tip of a very big commercial and moral iceberg.

Our email, like our postal mail and telephone conversations, should remain "sealed" (our coded information should not be decoded) unless the government can convince the courts that you or I might pose a threat and/or might be breaking the law. Therefore, no indiscriminate scooping of terabytes of citizen information should be allowed. Yet we already have this procedure in place: the Foreign Intelligence Surveillance (FISA) court. It is made up of 11 federal judges who decide (yes or no) on the intelligence services' applications for tapping phone lines and reading emails.

Did the FISA court give NSA permission to spy on Ms. Merkel? If not, who did? As best we can tell, the civil servants made this decision. The bureaucratic tail is wagging the political dog. Also troubling is this statement from NSA:

> The NSA calls its decryption efforts [breaking our codes to read our traffic] the "price of admission for the U.S. to have unrestricted access to and use of cyberspace."[4]

This statement reveals a mentality that I hope the readers of this report find unsettling. NSA is telling the world that the United States, with NSA acting as its proxy, has no restrictions on how it conducts itself in regard to information technology.

During my research for writing *The Nearly Perfect Storm: An American Financial and Social Failure,* I continued, time after time, to discover it was not for lack of law or authority that many of the problems associated with the 2008 meltdown came about. It was because of the incompetency of the people who were supposed to be doing their jobs, but did not.

While thinking about writing this essay, I decided to make the point that Congress and the White House have not been doing their jobs in protecting the privacy of American citizens. But the thought occurred that Senator Feinstein and her governmental colleagues have indeed been doing their jobs. Remember, she said, "…unless the United States *is engaged in hostilities* (my emphasis) against a country or there is an emergency need for this type of surveillance, I do

[3] Ibid.
[4] Michael Winter, "NSA Cracks Internet Security," USA TODAY, September 6-8, 2013, A1.

not believe the United States should be collecting phone calls or emails of friendly presidents and prime ministers."[5]

But this country is indeed doing just that. As later reports will show, the White House under both George Bush and Barak Obama pushed these programs. The United States has declared a never-ending war on terrorism. It's not a hot war. It's not a cold war. It's a warm war, one of just the right temperatures to keep citizens wary of enemies and accepting of the curtailment of civil liberties. Consequently, Senator Feinstein's statement justifies her seemingly ill-informed philosophy.

In today's world of asymmetrical war (nationless terrorism), we should not expect Uncle Sam to protect us if we do not give Uncle some latitude in how he goes about doing it. It must remain secret from us in order to keep it from our enemies. I accept this premise. But it must be subject to competent and rational oversight. And the seemingly innocuous collection of information of foreigners is far from innocuous:[6]

- The backlash in Europe over U.S. spying is threatening an agreement that generates tens of billions of dollars in transatlantic trade every year---and negotiations on other pacts worth many times more.

- A growing number of European officials are calling for the suspension of the "Safe Harbor" data-sharing agreement, which is vital to more than 4,200 American companies doing business in Europe, including Apple, Google, Facebook, and Amazon.

- Revelations of the extent of U.S. spying on its European allies is also threatening to undermine one of President Obama's top transatlantic goals: a sweeping free-trade agreement that would add an estimated $138 billion a year to each economy's gross domestic product.

In some situations, it would be impossible for U.S. businesses to serve European customers. Mark Zuckerberg, the chief executive of Facebook, puts it well:

> The government blew it. The government's comment was "Oh, don't worry, basically we're not spying on Americans." Right, and it's like, "Oh, wonderful, yeah, it like that's really helpful to companies that are really trying to serve people around the world and really going to inspire confidence in American Internet companies."[7]

America's Warm War has everyone in a hammer lock. Citizens, businesses, and government, well-intentioned or not, are on the mat.

A subsequent report will present several ideas, easily implemented on a PC, for keeping your mail secure…assuming the NSA has not yet succeeded in breaking current commercial encryption systems. Also, subsequent reports will provide non-technical tutorials on terms and

[5] Michaels and Madhani, "Uproar Could Spark," *USA TODAY*, October 31, 2013.
[6] Juergen Baetz, "EU Spying Backlash Threatens Billions in Potential US Trade," Associated Press, *The Desert Sun*, October 31, 2013, A6.
[7] Claire Cain Miller, "Angry Over U.S. Surveillance, Tech Giants Bolster Defenses," *The New York Times*, November 1, 2013, A1, A3.

 

concepts that I hope you will find helpful when you read about the important issue of Internet privacy.

Your on the Street Reporter

 