NSA Metadata Surveillance: Worth the Cost?

NSA Metadata Surveillance: Worth the Cost?

March 9, 2014

Hello from Your on the Street Reporter. This report continues the series on Internet privacy and security specifically, and privacy and security in America generally. The focus today is on the effectiveness or ineffectiveness of NSA's program of collecting information (metadata, as explained in earlier reports) on U.S. citizens' phone calls and Internet traffic.

To repeat: This writer supports government spying, but not in the matter it is presently being conducted. This report and others that follow will expand and elaborate on my point of view. My attitude is colored with an admittedly limited and dated exposure to America's government intelligence world, but one that is reinforced by my recent research of the views of government and non-government intelligence experts. (Please see the addendum to this report for a brief description of my work in the intelligence community.)

I offer this background information because these experiences led me to be skeptical of the federal government's intelligence apparatus. I found (and find) it bewilderingly inefficient and redundant. As one example, I read hundreds of the "super secret" National Intelligence Estimates (NIEs). Much of their information could be found in daily newspapers and were of marginal use.

One of my departments was not allowed to send certain military attaché reports to the CIA, the very agency responsible for America's overall intelligence operations. I asked the lead analyst of this department how the Defense Department could conceivably deny spy information to America's chief spy agency. He said he had no idea, but each member of this team had a "Military Eyes Only" stamp and they used it on many intelligence reports coming from the military officers stationed at embassies and consulates.

And for now: The situation with America's vast intelligence system is dismaying. We want terrorists caught before they do us harm. We want Uncle Sam to keep us safe from some dangerous people. We are willing to pay taxes to fund programs that will do just that. Yet how can we support a program in which millions of dollars are ploughed into a highly intrusive operation that yields practically no results?

The Washington Times (hardly a liberal news outlet) reported the following:

> Pressed by the Democratic chairman of the Senate Judiciary Committee at an oversight hearing, Gen. Keith B. Alexander [chief of the NSA] admitted that the number of terrorist plots foiled by the NSA's huge database of every phone call made in or to America was only one or perhaps two — far smaller than the 54 originally claimed by the administration.

Keep in mind that another NSA official outright lied to Congress about the program in the first place. He claimed the program did not exist. Later, he admitted he misspoke. Still, and somewhat contradictory, I do not question the good intentions of these people. This man likely

believes he lies for the good of us all. But I know enough about bureaucracies to understand, good or bad, they and their bureaucrats will self-perpetuate. It's human nature. Monks do not dissolve monasteries.[1]

"One or *perhaps* two." If I were in private business again and this specific operation were a company, a cursory cost-benefit analysis of this "business" would have me leaping to short sell its stock.

Yet, here is the hook that snarls the issue and catches a lot of fish (the fish being American citizens): What if those "one or perhaps two" cases saved America from at attack with weapons of mass destruction? How can anyone *not* defend such a program, however costly it may be?

I'll go out on a limb and say any effort of the magnitude of the use of unconventional weapons will not be discovered by tapping an unencrypted phone call or Internet email. The program might uncover a disaffected malcontent out to bomb a strip mall, but not a plot of major consequence.

But how can I be certain? I can't. Nor can you. Nor can NSA. Nor can anyone for that matter. It's the Black Swan conundrum. Very rarely does a black swan swim by. So, one does not plan for the black swan. But when it swims by, it swims by with devastating consequences. One in a billion of billion of chances. But what if that one in a billion of billion chances happens on the watch of our current intelligence gatekeepers. If you were one of those gatekeepers, what would you do? Show me the money, honey. If you don't fund my program, you're to blame, not me

Do we fund and staff for black swans? Can we afford to? If so, where does it end? Does it ever end? I have no answers to the questions. But I am disturbed that so much of America's intelligence operations operate behind closed doors. Not that they should be open to the public. Of course not. I am disturbed that even those who are legally responsible for being on the other side of those doors---protecting our security and our constitutional rights---are not doing their jobs. They had no idea of the extent of the NSA metadata operation. Now *that* is disturbing.

Again, I favor government spying, if it operates within the laws and courts. Otherwise, I am certain we will build, ever so incrementally, a society that routinely emasculates what the founders of this country (and subsequent Supreme Court rulings) considered vital to the human soul: privacy.

You may say, *I have nothing to hide*! So let me offer: Take a stroll on your favorite beach. Sit on your veranda enjoying a sunrise or sunset. Take a short pause to stop on your ride through Yellowstone. Walk the busy streets of London, jostled by fellow passersby but still enjoying the freedom of your own space. No one is intruding on your sanctity of just being unto yourself.

[1] "Washington NSA Admits Grossly Exaggerating Effectiveness of Mass Surveillance in Thwarting Terrorism," http://warincontext.org/2013/10/03/nsa-admits-grossly-exaggerating-effectiveness-of-mass-surveillance-in-thwarting-terrorism/.

These freedoms are going away. Cameras recording our everyday activities, including our veranda solitude. The data miners of this world are in the process of building a Big Data profile of just about everything we do.

Am I showing a bit of privacy paranoia? Perhaps, aside from my blog, books, and essays, I am one for solitude. I may be over reacting. But then, I Goggled my home address and downloaded aerial photos of my entire home, front yard, back yard, including my veranda. Luckily for Google googlers, I was not sunbathing on my deck. I'd hate to subject anyone to that scene.

Addendum

In the mid-1960s, I spent just under two years working as a Communications Officer in the U.S. Navy. I was posted to a two-star admiral communications flagship that sailed on the South China Sea during the Vietnam War. During this time, the United States fostered the removal (and unintended murder) of Ngô Đình Diệm, the president of South Vietnam. I followed aspects of this unfolding plot as I sat in the cryptography rooms in the ship.

I had an intelligence clearance that granted me access to and use of two separate cryptography departments on five different flagships of the U.S. Navy Seventh Fleet. One department was for Confidential, Secret, and Top Secret traffic. The other was for traffic beyond Top Secret. One aspect of this position was encrypting and decrypting messages flowing to/from Washington, the Seventh Fleet, the State Department, and the Pentagon. At that time, little did I realize I was witnessing history being made, and that I was a go-between in facilitating the exchange of parts of the documentation about these events.

I next served one year as a Logistics Officer. During this time, I went ashore onto Vietnam islands and beaches with Marines, UDT, SEALs, and South Vietnam Special Forces to "dislodge" Vietminh and Viet Cong.

I was then assigned to the Defense Intelligence Agency (DIA) at the Pentagon where I was in charge of three departments dealing with the dissemination of intelligence information coming from military attaches stationed at embassies, consulates, and other less obvious sites around the world. During this time, one of my ancillary jobs was the DIA "Librarian" of the National Intelligence Estimates (NIE). My department was responsible for sending NIEs to military units, based on need-to-know and prior authorization.

One of my departments did photo intelligence. I discovered the analysts had collected several thousand photographs of a Soviet spy airplane. (At least several thousand, we lost count.) I spent hours looking at what were essentially the same shots, just taken at different locations around the world. The various far-flung United States intelligence gatherers had been instructed several years ago to make sure they took shots of this plane at every opportunity. No one bothered to tell them enough was enough. Those who gave such orders were hesitant to do so because a new model of the plane might come along. I asked the lead analyst of the photo unit if perhaps the photo takers could be trained to tell the difference when/if a new model was flown. He smiled and said, "Mr. Black, that would require considerable training. We just tell them to shoot pictures of anything that has a red star on the tail." The practice was a forerunner to Big Data.

