Mathematicians Discuss the Snowden Revelations

This article is the latest installment in the *Notices* discussion of the National Security Agency (NSA). The previous installment, by Richard George, appeared in the August 2014 issue. A list of earlier articles appears there.

The author of the present article, William Binney, worked at the NSA for thirty years and left in October 2001 out of concern that the NSA was undertaking activities that were unconstitutional. Since then, he has become a prominent critic of the NSA. In July 2014, he appeared before the committee of the German Bundestag that is investigating the NSA. Further background can be found in, for example, "Bill Binney, the 'original' NSA whistleblower, on Snowden, 9/11 and illegal surveillance," by Fiona O'Cleirigh, *Computer Weekly*, June 2014, http://www.computerweekly.com/feature/Interview-the-original-NSA-whistleblower.

— *Allyn Jackson*
Notices *Deputy Editor*
axj@ams.org

The Danger of Success

William Binney

When I joined the Army Security Agency in the mid-1960s and later the NSA (National Security Agency) in 1970, I did so with the understanding that I would be working to defend the Constitution and help maintain the security of the US and the free world. For the first thirty years working in communications intelligence (COMINT), my job was to solve data systems, codes, and ciphers as well as analyze data used in communications of the Soviet Union and the Warsaw Pact. During this period, we had clear directions within NSA not to spy on Americans. These rules were documented in USSID-18 (United States Signals Intelligence Directive number 18), which we religiously followed.

In the 1990s, in addition to being the co-founder of the Signals Intelligence Automation Research Center (SARC), I became technical director of the NSA's World Geopolitical & Military Analysis and Reporting Group, which employed around 6,000 people. In this position, I had to focus on issues dealing with public communication. I had to help resolve the problems of dealing with the vast amount and verity of communications. The problem, simply put, was: How can one smartly select relevant data from the huge flow going across the fiber optic lines around the world? These communications were primarily in two networks: the Public Switched Telephone Network (PSTN) and the World Wide Web (WWW).

The PSTN system is uniquely numbered (that's how caller ID works) and much easier to deal with compared to the WWW. In the WWW, we had to first solve the problem of reconstructing the data going across the fiber lines. This meant we had to process data at 155mbs—the rate of one fiber. We achieved that in 1998. From then on, it was possible to acquire all the data on a fiber. Space and computing power determined how many fibers we could collect. Once all that data is captured it was, and still is, extremely important to smartly select relevant information for analysts to review. This was a major problem for analysis back in the 1990s, and, from all indications, today it is even more of a problem. My small team developed arguments that selected material based on a defined zone of suspicion around known and targeted entities, plus some other target-specific properties.

Building relationships between entities was at the foundation of the analysis process that made it possible to smartly select data. We could select a rich set of data for analysts to look at and then let the rest of the data go without collecting it. This would give privacy to most of the people in the world. In this process, we could capture

William Binney is a former NSA technical director, now retired. His email is williambinney0802@comcast.net.

DOI: http://dx.doi.org/10.1090/noti1168

communications of Americans. So I designed a logic that would encrypt the attributes of any US citizen pulled into the collection. These protected attributes would not be decrypted until "probable cause" was developed and presented to a court for a warrant. A warrant had to be requested within seventy-two hours of starting to examine a US entity; otherwise, the collection had to be stopped and the data purged from the database. This process, we believed, was constitutionally acceptable, legal according to FISA (Foreign Intelligence Surveillance Act of 1978), and consistent with Executive Order 12333 (which dates from the 1980s and deals with surveillance outside the purview of FISA).

There are other benefits from smart selection of data. Since only a fragment of the data flow would be captured, there would be no need to build storage facilities like the one NSA completed in 2013 in Bluffdale, Utah. Nowhere near the number of contractors or contracts would be necessary to maintain the data and programs associated for tasks like query and information distribution. Plus, of course, analysts would not be buried in data from daily pulls for target information, which means they would have a much higher probability of finding actionable intelligence.

Unfortunately, all this power to capture data, graph social networks, and index collected data to the relationships in the graph was directed initially inward, toward US citizens. This automatically produced a profile of the activity of everyone. This profile was available on request from analysts. Also, in the process, the NSA removed the privacy protections for US citizens and decided to collect and store as much data as it could ingest. No one had privacy from the government anymore. I of course objected, as in my mind these actions were, at a minimum, a violation of the First, Fourth, and Fifth Amendments to our Constitution.

The First Amendment was violated because the graphing of social networks (enhanced by other knowledge bases—for example, a reverse lookup of the phone book) would show the people you are associated with. The First Amendment says you have the right to peaceably assemble, and the Supreme Court has held (e.g., in NAACP v. Alabama) that the government does not have a right to know with whom you are assembling. The collection of your email, chatter, and phone calls (recorded or transcribed) is a violation of the Fourth Amendment right to be secure in your affairs. And using content data in order to search for criminal activity can be a violation of the Fifth Amendment, which gives the right not to be a witness against yourself. An example of this is the "parallel construction" techniques used by the FBI and the DEA's Special Operations Division, to find evidence to submit in court proceedings when they use data collected by the NSA (see "Exclusive: U.S. directs agents to cover up program used to investigate Americans," by John Shiffman and Kristina Cooke, *Reuters*, August 3, 2014). The procedure, as outlined in the *Reuters* article, instructs agents not to let the court or lawyers involved in the case know about the NSA data. So, they perjure themselves. This I call a planned programmed perjury policy run by the Department of Justice.

Some have claimed that the NSA collection is innocuous, because, for those who are not terrorist suspects or associates, the NSA collects only metadata, such as telephone numbers, the date, time, and duration of telephone calls. Evidence that this claim is untrue can be found, for example, in the testimony of two NSA transcribers who worked at Fort Gordon in Georgia—Adrienne Kinne and David Murfee Faulk. They have testified that after the invasion of Iraq they transcribed, in full, calls made by US citizens in the Green Zone—members of the military, employees of NGOs, journalists, etc.—to their families back in the US. Kinne and Faulk both were disturbed at having to transcribe these intimate, personal conversations between family members who were separated because of the war. This transcribing was done without a warrant and thereby violated both USSID-18 and FISA—plus of course the Constitution.

So you see what happens when a technical advancement is made. Politicians and bureaucrats, when given the power the advancement provides, use it. Herein lies the danger that seems to be a failing of humankind, as it has happened over and over again down through history. We just don't seem to learn from it. Even with the exposure of the Snowden material detailing the extent of bulk data acquisition, our Congress and the Administration still don't appear to have the stomach to ensure that the activity of NSA and the other intelligence community agencies is verified. In other words, they prefer to trust and not verify. Unless we strongly object to our representatives in Washington, we don't stand a chance of recovering our Constitutional rights.