Mathematicians Discuss the Snowden Revelations

The following article was solicited as part of the *Notices* discussion of the National Security Agency. The previous installment in the discussion appeared in the June/July 2014 issue of the *Notices* and included articles by Keith Devlin of Stanford University and Andrew Odlyzko of the University of Minnesota. Those articles were preceded by an introduction that describes how the discussion came about and provides a list of previous *Notices* pieces on this topic, as well as citations to articles that have appeared in other publications. Since then, additional coverage has appeared in the media. On June 7, 2014, the BBC aired a radio story, "Are science and spying connected?", by Gordon Corera. On June 5, 2014, *Forbes* online magazine published an article, "Mathematicians Urge Colleagues to Refuse to Work for The NSA", by Kashmir Hill. Both the BBC broadcast and the *Forbes* article featured interviews with mathematicians, and the latter mentioned the *Notices* discussion.

Other material has appeared on the Web. For example, on May 14, 2014, the International Association for Cryptologic Research issued a statement about mass surveillance: `http://www.iacr.org/misc/statement-May2014.html`. Earlier, in January 2014, "An Open Letter from US Researchers in Cryptography and Information Security" appeared on the Web; see `http://masssurveillance.info`. Since November 2013, Tom Leinster of the University of Edinburgh has moderated a discussion of these issues, with a focus on Britain's GCHQ (Government Communications Headquarters), in n-Category Cafe blog (`http://golem.ph.utexas.edu/category/`).

As we have collaborated on organizing this discussion, we had the impression that mathematicians are hesitant to voice their opinions on this topic. We hope to hear further opinions on this important topic in the future. Unsolicited articles are welcome. Inquiries and submissions may be sent to `notices-snowden@ams.org`. Articles of 800 words or less are preferred. Those of 400 words or less can be considered as Letters to the Editor and should be sent to `notices-letters@ams.org`.

—Michael Harris
Institut de Mathématiques de Jussieu
`harris@math.jusseiu.fr`
Columbia University
`harris@math.columbia.edu`

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

DOI: http://dx.doi.org/10.1090/noti1156

NSA and the Snowden Issues

Richard George

As a mathematician who worked for the National Security Agency for 41 years, I truly appreciate the American Mathematical Society having this open discussion about a very important topic. At NSA, my entire career was on the information assurance side—white hat—evaluating equipment used to protect U.S. information.

One of the tasks I really enjoyed at NSA was being able to work closely with NIST (National Institute of Standards and Technology) on the evaluation of both the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES); AES is the symmetric algorithm widely used by government, industry, and private citizens to ensure confidentiality. It is a major component of Suite B along with elliptic curve cryptography. Suite B (a set of algorithms and protocols for encryption, key exchange, hashing, and signature) is important

Richard George worked for the National Security Agency for 41 years before retiring in 2011. Currently he is Senior Advisor for Cyber Security at the Johns Hopkins Applied Physics Laboratory.

for international interoperability needs and also enables the government to choose cost-effective commercial security devices to provide protection for classified information. It ensures that strong cryptography is affordable and available to everyone. These were challenging and exciting tasks; problems like these make NSA a great place for mathematicians. The talk about NSA weakening crypto reminds me of the 1970s when the popular line was that "the DES S-boxes don't look like a random set, so that's where the back-door is". Of course they weren't random—they were much stronger than a typical random set as Adi Shamir later showed. As I said at the RSA Conference in 2011, I don't think NSA was clever enough to hide a weakness in crypto that people like Whitfield Diffie and Adi Shamir wouldn't find. And I have never heard of any proven weakness in a cryptographic algorithm that's linked to NSA; just innuendo.

I was not a direct part of the signals intelligence (SIGINT) system, but the math community at NSA is very open; techniques and research are openly shared throughout. As an NSA employee, I was aware of the rules about signals intelligence. When public discussions about foreign intelligence take place, there are some facts about the SIGINT system that people need to know:

- NSA is a supplier of intelligence, not a consumer
- NSA does not choose its targets
- NSA activities and processes are driven by laws established by Congress and by directives from the President, the Secretary of Defense, and the Director of National Intelligence (DNI).

NSA's intelligence activities stem from a foreign-intelligence requirement—initiated by one or more Executive Branch intelligence consumers (the White House, Department of State, Department of Defense, etc.), vetted through the Justice Department as a valid need—and run according to a process managed by the Office of the Director of National Intelligence. When NSA receives those requirements, NSA's analysts look at what's known as the "information need" and determine the best way to satisfy it. That process involves identifying the foreign entities that might have the information, researching how they communicate, and figuring out how best to access those communications in order to acquire the information. The General Counsel of NSA validates that NSA has the authority to carry out the planned activities. The number of requests for information that the NSA receives from the various government entities is huge: in 2012, the requests filled 36,000 pages.

Many of the foreign threats that NSA must monitor to protect our safety and security operate in the same environments and use the same technology as innocent persons. It is NSA's responsibility to find effective and lawful ways to gain access to these communications by foreign targets while protecting the privacy and civil liberties of individuals who occupy the same space or employ the same technology.

NSA does not collect and exploit a class of communications or services that would sweep up communications that don't have information of bona fide foreign intelligence interest. The result of each task that NSA carries out is intelligence that is passed to the group that requested it.

Phone metadata (section 215 of the Patriot Act) has been in the news a great deal since last summer's unauthorized disclosures. Many of the claims about this metadata program were not really true. Under Section 215, the government stored in bulk metadata related to telephone calls. As President Obama said in January, the U.S. government believes this is a capability that must be preserved, and noted that independent reviews did not turn up any indications that the program had been intentionally abused. However, changes were ordered to enhance public confidence; specifically, the president ordered a transition to end the bulk metadata program as it existed, and the establishment of a program that preserves the capabilities the government needs without the government holding the data.

I've heard some knowledgeable people claim that this metadata can be used to create detailed profiles of people. Of course, that's not true. Data is used to create profiles—that's why when I check the weather on the Internet, I get ads for hotels in cities I've looked at or ads for flights to those cities. Big business has already created profiles on us from all the data that is readily available. The only thing metadata alone can be used for is to point to interesting phone numbers; then data can be used to get other information. I find it ironic that no one seems concerned that Big Industry already has the type of profile on Americans that we worry that the government might create. I guess there's no concern that a Big Industry employee might ever misuse the information.

The issue of privacy in all this is very interesting. The folks I knew in SIGINT, and I knew them very well, would not dream of violating U.S. citizens' rights. Please keep in mind that there may be a few bad apples in any set of people who would do something inappropriate, but they would be a minuscule minority. That's true everywhere, though we'd like to think background checks help somewhat at NSA and that people come to work for NSA out of a desire to protect the nation, the citizens, and our way of life. In fact, NSA officials and employees have given up much of their own privacy to accomplish their mission. Each year they disclose to the government their financial dealings and status, grant the government the right to access any and all banking records, grant the government the right to monitor phone calls and emails on their office systems, and submit to a full background check and polygraph every five years. More importantly, they are fully aware that they are targets of foreign intelligence services that will be watching for any weakness that can be exploited. When I was at NSA, we all knew that a government was likely listening to all our phone calls—just not the U.S. government.

Every time an espionage incident happens—John Walker, Aldrich Ames, Bradley Manning, Edward Snowden—in which someone with a clearance has signed an oath to not disclose information and then violates that oath and trust, it comes as a disappointment, a feeling of betrayal by someone in the family. It hurts NSA and it hurts the country. We are all aware that untrustworthy individuals will continue to crop up, but it's still a shock. System administrators occupy key positions today, much as crypto custodians, the holders of the keys (Walker), did years ago. The damage that such a person can cause to an agency is immense. The trust that is damaged, both within our own country and with other countries as well, will take years to rebuild.

Finding intelligence in the mountain of data that exists today is a monumental task. If it was simple, we would predict all the terrible events that happen—9/11, Boston Marathon bombing, etc.—but it's not. There is much publicity on events that happen and none on those that are stopped. NSA is just one player on the team—from the Department of Homeland Security, FBI, Drug Enforcement Administration, Coast Guard, Air Force, Army, Navy, Marines, to local police and fire departments—whose reason for existence is to protect the people of this nation. Events like the Snowden leaks make that effort harder.

Whether the rules should be changed further is a great topic for debate. What is already clear, however, is that the threats are not easing. And they are not going to go away.

Lusztig Awarded Shaw Prize

George Lusztig

On May 27, 2014, the Shaw Foundation announced the awarding of the 2014 Shaw Prize in Mathematical Sciences to George Lusztig of the Massachusetts Institute of Technology "for his fundamental contributions to algebra, algebraic geometry, and representation theory and for weaving these subjects together to solve old problems and reveal beautiful new connections." The prize carries a cash award of US$1 million.

The Shaw Prize in Mathematical Sciences Committee released the following statement about Lusztig's work.

"For more than two hundred years, symmetry groups have been at the center of mathematics and its applications: in Fourier's work on the heat equation in the early 1800s; in Weyl's work on quantum mechanics in the early 1900s; and in the approach to number theory created by Artin and Chevalley. These classical works show that answers to almost any question involving a symmetry group lie in understanding its realizations as a group of matrices; that is, in terms of its representations.

"Starting with his early work in the 1970s and 1980s, in part jointly with Deligne, Lusztig gave a complete description of the representations of finite Chevalley groups, these being the building blocks of finite symmetry groups. The Deligne-Lusztig description uses the topology and geometry of Schubert varieties. The latter were introduced in the nineteenth century as a tool to count solutions of algebraic equations.

"The vision of this work is that the algebraic subtleties of representation theory correspond perfectly to the geometric/topological subtleties of Schubert varieties. This vision has grown into a broad and powerful theme in Lusztig's work: he has shown that many central problems in representation theory—including those of real and p-adic Lie groups, which are the language of applications from number theory to mathematical physics—can be related to topology and geometry by means of Schubert varieties. This idea is at the heart of many exciting recent developments, for example in progress toward the Langlands programme in automorphic forms.

"Representations are complicated, as are the Schubert varieties to which they are related. Beginning in a 1979 paper with David Kazhdan, and

DOI: http://dx.doi.org/10.1090/noti1154