Editor's Note: This article first appeared in French translation in the journal *Commentaire*, No. 149, Spring 2015, which appeared on March 11, 2015. The translation was done by Isabelle Hausser of *Commentaire*. Below is the original English version, which was done as an independent research project by the author under the auspices of the International Security Program of the Harvard Kennedy School's Belfer Center for Science and International Affairs.

They Believed They Were Doing No Wrong: NSA and the Snowden Documents

Charles G. Cogan

Introduction

I became involved with this study after attending a conference sponsored by the Association of Former Intelligence Officers (AFIO) in northern Virginia in the spring of 2014. The keynote speaker was John Hamre, a respected former civil servant who at one time had been Under Secretary of Defense. He is now president of the prominent Washington think-tank, The Center for Strategic and International Studies.

Hamre spoke with some passion about what he considered the unjust treatment of National Security Agency (NSA) and other officials by the press and by extension the public, in the wake of the Edward Snowden disclosures; whereas the reality was that they were not only doing their job but doing it in conformity with the legal authority under which they were working.

When I placed Hamre's remarks against the charges leveled by the American Civil Liberties Union (ACLU) and by journalist Glenn Greenwald, who had helped publish Snowden's collection of stolen documents, as well as by other individuals, I said to myself, somewhere between these two very discrepant points of view must lie something close to the truth. I leave it to the reader to judge whether my effort to be as objective as possible on this highly-charged issue is credible.

Additionally, I thought that, given the complexity of the subject and the confusion surrounding it, it would serve a useful purpose for the general public to become better acquainted with it. Hence another objective of this study.

At the conclusion of this research, and to summarize my bottom line, I would say that the NSA, while operating under the direction of higher authority, nevertheless had a mindset—typically American—of overdoing things and with it, a reflex of protecting the secrets of the organization. As the previous director of the NSA, Gen. Keith Alexander, was fond of putting it, "We collect everything." President Barack Obama himself acknowledged in an interview with David Remnick, that the NSA had "too much leeway to do whatever it wanted or could."

But by the same token, the President also told Remnick, "I actually feel confident that the way the NSA operates does not threaten the privacy and constitutional rights of Americans and that the laws that are in place are sound, and, because we've got three branches of government involved and a culture that has internalized that domestic spying is against the law, it actually works pretty well" (*The New Yorker*, January 27, 2014, p. 60).

Overall, it is ironic, that with such a toxic subject—NSA spying on Americans and non-Americans—NSA and its critics seem to have come out in the right. As the outgoing deputy head of the NSA, John Inglis, stated in an interview on National Public Radio on January 10, 2014, with *Morning Edition* co-host Steve Inskeep, "The accusations of misbehavior…have not been borne out…The presidential review group recently concluded that there have been no illegalities or abuses by NSA…It is not an accident that there's not been a foreign-induced terrorist attack on this nation's soil in the last 12 years." (N.B. The presidential review group was formally named the Director of National Intelligence Review Group on Intelligence and Communications Technologies.[i] It included Chair Michael Morell, former deputy CIA director; Richard Clarke, former counter-terrorism coordinator in the White House; Professor Geoffrey R. Stone of the University of Chicago Law School; Professor Cass R. Sunstein of Harvard Law School; and Peter Swire, President Bill Clinton's privacy director).

As Inglis further observed in the same interview, there is a need to "rebalance the balance we have struck between security, secrecy and transparency…we need to continue to move in the direction of having greater transparency about the nature of NSA… Our European counterparts say that when you try to achieve the right balance between security and privacy, you need to think in terms of necessity and proportionality…We have struck a good balance between security and the defense of civil liberties. [The] presidential review group said that as opposed to… pre-1978 there's a stark contrast[ii]…we cannot run the risk of giving away all of our capabilities in the spirit of trying to make ourselves completely transparent…I don't think we can afford to give those capabilities away to our adversaries." (N.D.L.R. I should add that the interview Inglis had with Inskeep was the most

important of the many sources I consulted, a list of which is contained in the Annex).

What is NSA Surveillance?

Within NSA, the surveillance or collection program to deal with the threat of terrorism is known as "The Project." In analyzing "The Project," the first distinction to be drawn is between "content" and "data." In NSA parlance, the term data does not encompass the content of messages. The second distinction to be drawn is between the telephone and the Internet.

"The Project" includes both the collection of content and of data, the latter known as "metadata" in its telephone context. There was a similar program to collect metadata from electronic communications (emails, etc.) but this idea was abandoned in late 2011 because it was too hard to make operationally workable, too difficult to comply with the safeguards, and too costly. "We don't collect email metadata." (Inglis 2014)

The trail begins with the Foreign Intelligence Surveillance Act of 1978, which was the result of the Church and Pike hearings in the U.S. Congress in the early 1970s, the declared object of which was to investigate, among other things, certain excesses of the Central Intelligence Agency (CIA). In addition, Luke Harding, author of *The Snowden Files*, refers to "a series of reports by the Senate Committee, led by Frank Church, into unforgivable domestic abuses: the FBI's harassment of Martin Luther King, CIA assassination programs, and the watch-listing of 75,000 Americans." (Harding, 2014, p. 531). Harding also mentioned the following: "[President Nixon ordered] the NSA to tap the phones of several fellow Americans he didn't like,

under the notorious MINARET program. The MINARET scandal brought about the Foreign Intelligence Surveillance Act [of 1978]. Under it, the NSA was supposed to steer clear of communications inside the U.S. or involving Americans, unless it had a warrant." (Harding, 2014, p. 164).

The FISA Act prescribes procedures for physical and electronic surveillance and collection of foreign intelligence information between foreign powers and agents of foreign powers (which may include U.S. citizens suspected of espionage or terrorism). The law does not apply outside the United States It has been amended several times since 9/11. The law has been since amended to apply outside the United States.

I. The telephone metadata program under the 215 Authority

The metadata program, which authorizes the collection of telephone metadata only, is conducted under the 215 Authority, that is, Article 215 of the Patriot Act of October 26, 2001, which is an amendment of the FISA Act of 1978. Section 215 authorizes the FBI to collect a wide variety of data without the knowledge of the source. The NSA applied this authorization to the collection of telephone metadata, that is, data surrounding the fact of the message itself, i.e. telephone numbers [that both originate and receive calls], the time and date of the call, and the duration of the call. The government stores this bulk telephonic metadata for a period of five years, after which it is destroyed. The 215 authority was not considered as allowing the government to listen in on anyone's telephone call, not even a terrorist. (Inglis June 18, 2013 congressional testimony).

On the level of implementation (as opposed to authorization), and just prior to the signing of the Patriot Act, President George W. Bush on October 4, 2001, had given his approval to what was called the Terrorist Surveillance Program," otherwise known under its code name, "Stellar Wind." This included the wholesale collection of Internet and telephone metadata and other communications. The program had to be recertified by the Attorney General every forty-five days. It was only in March 2004 that Attorney General John Ashcroft and his new deputy James Comey refused to recertify the program which, upon reflection, they considered as violating the Fourth Amendment and the original Foreign Intelligence Surveillance Act of 1978. The program came to a temporary halt.

The telephone metadata program was designed to cover a seam exposed in the 9/11 attacks. The program would allow the U.S. Government to detect communications between terrorists operating outside the United States who are themselves communicating with potential terrorists inside the United States As Inglis put it, "The NSA could see that one end of a communication was at a safe house overseas but did not have the means to determine that the further end of it was actually in the United States of America. So the 215 metadata program is essentially designed to cover a seam that we don't know any other way to cover." (Inglis 2014) (In other words the program permits the creation of a capability to find something that is the connection of a foreign plot to a domestic extension of that plot.)

Inglis drew the example that the NSA knew things prior to 9/11 about terrorist conspiracies overseas that had not been tied to activities in the United States , and he cited without elaboration the al-Midhar case. (Al-Midhar was one of two

9/11 terrorists whose meeting had been monitored in Southeast Asia but then they had moved to California where their movements had not been followed. At no time did they give indications of a plot on 9/11).

The metadata stored under the telephone program may be queried for content only when there is a "reasonable articulable suspicion" that an identifier (i.e. a telephone number) is associated with specific foreign terrorist organization.

In 2012, according to the presidential review group that looked into NSA's operations, NSA went to the metadata 288 times for particular telephone numbers. This meant a "reasonable articulable suspicion" about these numbers existed. With two stages of numbers that were called from that number (so-called "hops"), it amounted to 6,000 in 2012. No names, no content, no locational data. Just numbers. (Inglis 2014)

According to Inglis, it is hard to pin down the effectiveness of the 215 Authority (the telephone metadata authority). There may have been one case that was exposed, in San Diego. However, Inglis' interviewer (Inskeep) pointed out that the presidential review group did not even validate that one, and he questioned whether the metadata program was worth its tremendous political cost. But Inglis countered by saying, "the question remains as to whether you're going to have a capability to find something that is the connection of a foreign plot to a domestic extension of that plot." Inglis did acknowledge that "The government doesn't need to hold the data, it could be held by a third party." (Inglis 2014).

II. The Section 702 Program

A second program is authorized under Section 702 of the Foreign Intelligence Surveillance Act (FISA), as amended in 2008. This FISA Amendments Act (FAA) of 2008 authorizes access to the content of electronic communications of foreigners who are themselves not within the United States, for foreign intelligence purposes. (Section 702 of the FISA Amendments Act of 2008 (FAA)—directed against non-U.S. persons.)

The 702 program involves the compeled assistance of an electronic communications service provider. In specific terms, it consisted of agreements between NSA and nine of the biggest Internet companies, namely AOL, Dropbox, Google, Apple, Yahoo!, Linkedin, Twitter, Microsoft, and Facebook. Access to these Internet companies falls under the code name "Prism."According to Inglis, "The vast majority of [the 54 plots discovered by the NSA] were uncovered using what's called the 702 Authority, what has been sometimes referred to as Prism."(Inglis 2014).

According to Harding, "The top secret PRISM program allows the U.S. intelligence community to gain access to a large amount of digital information—emails, Facebook posts, and instant messages. (Harding, 2014, p. 360).

The so-called "incidental" or "back door" or "reverse" identification of a U.S. person involves the hypothetical example of al Qaeda leader Ayman al-Zawahiri telephoning someone in the United States. The statements of the U.S. person should be screened out unless they are important to the intelligence value of the communication. If they are important, one would still have to get a warrant to investigate this U.S. person. The effect of the FISA Amendments Act of 2008 was

such that for a U.S. person, one can no longer get authorization from the Attorney General; it must be from the FISA Court. In his interview with Inskeep, Inglis stressed that, "In order for [NSA] to target the content of an American's communications [it] needs a court warrant" and "the 702 provision [says] that we cannot use our authorities under what's called the Prism program to reverse-target Americans". (Inglis 2014).

The New York Times, in an article on July 3, 2014 (p. A9), reported on a comparison between the 215 and 702 programs that had been made by the Privacy and Civil Liberties Oversight Board. The article is contained in the following paragraphs.

"The Board, which Congress made an independent agency in 2007, stated in a report of 1 July 2014 that NSA's exploitation of Internet connections in the United States to monitor foreigners communicating with one another abroad is largely in compliance with both the Constitution and the surveillance law that Congress passed six years ago. This refers to the 2008 amendment of the Foreign Intelligence Surveillance Act. [Note: earlier the Board had criticized the collection by the NSA of phone records of Americans.] Current legislation which has passed the House [the FISA Improvements Act] and is pending before the Senate deals largely with the phone call records program. That program involved the Agency's retention of billions of records for all phone calls made to or from the United States. Under the new legislation, telecommunications companies would retain these records, and NSA would have access under court orders.

"The Board's report of 1 July deals with what NSA refers to as "702 collection", a reference to Section 702 of the amended FISA Act of 2008. This amendment took place after

the NYT revealed a program of warrantless wiretapping that began after 9/11."

"The Board's report stated that, "The Section 702 program has enabled the government to acquire a greater range of foreign intelligence that it otherwise would have been able to obtain and to do so quickly and effectively.

"While the Board found little value in the bulk collection of Americans' telephone data [the 215 program], the 702 program, aimed at foreigners "has proven valuable in the government's efforts to combat terrorism as well as in other areas of foreign intelligence." The program is also used to track nuclear proliferation and to monitor the phone calls and emails of foreign governments and their leaders."

Note: In December 2013, Federal Judge Richard Leon ruled that the [NSA's] bulk collection of Americans' telephone records probably violated the U.S. Constitution. (Harding, 2014, p. 547).

III. The "Five-Eyes" Issue

There is a separate type of collection that comprises the penetration of fiber optic cables to obtain content, as these fiber optic cables pass through the United States. As Inglis put it:

> It might be surprising to someone that a communication that makes its way from, say, some ungoverned space in the north of southwest Asia to a place like Yemen sometimes transits through the United States of America. It might then be available for review by a foreign

intelligence organization like the National Security Agency. (Inglis 2014).

This relates to the so-called "Five Eyes" issue that stems from the US-UK SIGINT Agreement of 1946, which mandated a free exchange of signals intelligence. It was later extended to Canada, Australia, and New Zealand and was characterized as the "Five Eyes." Informally it was agreed among the five not to spy on each other. The fact that it was informal apparently gave President Obama the justification for saying publicly that the United States had no actual agreement not to spy on other countries.

As Luke Harding wrote about the system, "Together with GCHQ [the British counterpart of NSA], the NSA had secretly attached intercepts to the fiber-optic cables that ringed the world. This allowed the U.S. and UK to read much of the globe's communications. (Harding, 2014, p. 26). Elsewhere, Harding wrote of the NSA's "highly sensitive cable-tapping program, [run] parallel to GCHQ's British TEMPORA project and was codenamed UPSTREAM. It gives the NSA direct access to the fiber-optic cables carrying internet and telephone data into, out of, and around the U.S. (Harding, 2014, p. 365).

As is clear from the above, these programs included only Anglo-Saxon countries, or what is sometimes referred to as the "Anglosphere." In 2010, I wrote an article for the French journal *Commentaire* on the attempt by the erstwhile Director of National Intelligence, Admiral Dennis Blair, to extend a "no-spy agreement" beyond the Five Eyes to France. Blair seems to have concluded that other major Western allies should be included in such an agreement. His onward intention was to extend such an agreement to Germany as well.

However, Blair proposed to put the agreement with the French in writing, whereas within "Five Eyes," there was nothing in writing about not spying on each other.

Blair made his proposal on France after the then French President, Nicolas Sarkozy, had turned French-U.S. relations around, presumably for good. Sarkozy had thrown himself at the feet of the U.S. Congress when he declared before that body on November 7, 2007, "I want to be your friend."

But in the final analysis, the White House turned down Blair's proposal, presumably thinking that a future French government might not be quite as pro-U.S. as M. Sarkozy's was.

So the major European allies of the United States remain outside the "Five Eyes" arrangement. In the summer and autumn [of 2013], *Guardian* US published several notable scoops, based on the Snowden revelations. It revealed that the NSA was spying on thirty-five world leaders…(Harding, 2014, p. 514), most notably French President François Hollande and German Chancellor Angela Merkel. The French protest was more or less *pro forma*, as the French had a history of spying on the United States, notably American business travelers to Paris.

But the reaction of the Germans, which did not have a vigorous program of spying on the United States , and who had a history of Nazi and Stasi intrusion into private lives of German citizens, was quite different, especially since Merkel's private cellphone had been tapped. As Luke Harding wrote, "*Der Spiegel* found [Angela] Merkel's mobile number on an NSA docuent provided by Snowden. Her number featured next to the words: 'GE Chancellor Merkel'. The document, S2C32, came

from the 'European States Branch' of the NSA's Special Collection Service (SCS)." (Harding, 2014, p. 476)

After these revelations, the Germans sent a political-level delegation to Washington to ask for a no-spy agreement. This was refused, and the Germans left the discussions. In contrast, the French sent an intelligence-level group to Washington for informal talks on the subject.

Also in the aftermath of these revelations, and according to Inglis, "the president… asked…about whether or not we should favor some greater degree of outreach between [allied] organizations, in much the same way that we have for 70 years between the English speaking nations known as …the Five Eyes [The U.K., Australia, New Zealand, Canada and the U.S.]. Should we extend that same degree of greater collaboration to others?...And I think that's a question we're actually walking our way through." (Inglis 2014)

In its Recommendation 21, The presidential review group stated the following:

> We recommend that with a small number of closely allied governments, meeting specific criteria, the U.S. Government should explore understandings or arrangements regarding intelligence collection guidelines and practices with respect to others' citizens (including, if and where appropriate, intentions, strictures, or limitations with respect to collections). The criteria should include:
>
> (1) shared national security objectives;

(2) a close, open, honest and cooperative relationship between senior-level policy officials; and

(3) a relationship between intelligence services characterized both by the sharing of intelligence information and analytic thinking and by operational cooperation against critical targets of joint national security concern. Discussions of such understandings or arrangements should be done between relevant intelligence communities, with senior policy-level oversight. (review group report, p. 40)

* * *

Notes

[i] In response to recommendations of a bipartisan national commission formed to examine the Intelligence Community in the wake of the 9/11 attacks, Congress in December 2004 passed the Intelligence Reform and Terrorism Prevention Act (PL 108-458). The law established an Office of the Director of National Intelligence to head the intelligence community.

[ii] For mention of the Foreign Intelligence Surveillance Act of 1978, see p. 4.

ANNEX : List of Principal Sources

Glenn Greenwald, *No Place to Hide* (New York: Henry Holt, 2014)

Luke Harding, *The Snowden Files* (New York: Vintage Books, 2014)

John Inglis, interview on National Public Radio on January 10, 2014 with *Morning Edition* co-host Steve Inskeep

Inglis, June 18, 2013 congressional testimony

Presidential Review Group Report (Director of National Intelligence Review Group on Intelligence and Communications Technology)