Written Remarks for the German Parliament Committee of Inquiry

June 26, 2014

Christopher Soghoian, Ph.D.
Principal Technologist,
Speech, Privacy & Technology Project
The American Civil Liberties Union[1]

Introduction

Members of the committee, thank you for the invitation to testify before you today. I regret that I am not able to do so in person, due to a mechanical problem on my scheduled flight to Germany, but I hope to have the opportunity to do so at another date in the future.

In these written remarks, I will present my views on several topics related to surveillance. The main point I wish to make is this: The German government must prioritize information security if it wishes to protect itself, German companies, and the German people from surveillance by sophisticated foreign governments. This will require more than just establishing a "German cloud". Prioritizing security will also mean that the German police and intelligence services will also lose the ability to monitor phone calls, emails and cloud stored data that they likely will argue is essential to their work. To summarize: to keep the NSA from watching, you must also keep your own police and intelligence services from watching too.

The Limitations of Data Sovereignty

Even before the disclosures to the media in 2013 by Edward Snowden, European scholars had issued warnings about the FISA Amendments Act Section 702, and the ease with which it permitted the US government to compel US companies to provide data about their foreign customers.[2] After the media revealed the existence of PRISM, officials in several countries, including Brazil and Germany, voiced their concern about their countries' exposure to NSA surveillance. Germany's Interior Minister Hans-Peter Friedrich advised people who did not wish to have their communications monitored to "use services that don't go through American servers,"[3] while EU Commission Vice President Viviane Reding suggested that it was time for "Europeans to build their own cloud."[4]

European companies also seized the opportunity to use the NSA spying controversy to advertise their products. German email providers T-Online, GMX and web.de launched the "Email Made in Germany" program, which promised users that emails traveling between the three companies would never exit Germany.[5] Although it is of course always a good thing when companies improve the security of their

[1] The opinions expressed in this testimony are my own alone.

[2] *See* Joris Van Hoboken, Axel Arnbak and Nico Van Eijk, Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad, June 9, 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103.

[3] *See* German Minister: Drop US Sites If You Fear Spying, Associated Press, July 3, 2013, http://bigstory.ap.org/article/german-minister-drop-google-if-you-fear-us-spying.

[4] See Michael Scaturro, The Quest to Build an NSA-Proof Cloud, The Atlantic, November 21, 2013, http://www.theatlantic.com/international/archive/2013/11/the-quest-to-build-an-nsa-proof-cloud/281704/.

[5] *See* Boom Triggered By NSA: German Email Services Report Surge in Demand, Spiegel Online, August 26, 2013, http://www.spiegel.de/international/germany/growing-demand-for-german-email-providers-after-nsa-scandal-a-918651.html.

products, the modest security measures announced by European companies to date, and the proposals for a “European cloud” from EU leaders will have a limited impact on the ability of the NSA or other well-resourced intelligence agencies to spy on Europeans.

These proposals assume that the only way that the NSA can monitor the communications of Europeans is by watching the data as it crosses international fiber optic cables, or demanding a copy of it it once it is stored on the servers of US companies. It is certainly true that the NSA and its 5-eyes partners engage in bulk collection of communications that flow through international communications cables they are able to access. It is also true that the NSA (through their friends at the FBI) are able to compel US cloud computing companies to turn over data in their possession. However, these are not the only ways for the NSA to get data.

When Britain's intelligence service, GCHQ, accessed the internal networks of Belgian telephone network operator Belgacom, they did so by hacking into the Belgian company.[6] Similarly, when GCHQ penetrated the networks of German satellite companies Stellar, Cetel and IABG, they did so by hacking.[7] The NSA's own hacking unit, the Tailored Access Operations (TAO) division, is reportedly “the largest and arguably the most important component of the NSA's huge Signal Intelligence Directorate, consisting of over 1,000 military and civilian computer hackers, intelligence analysts, targeting specialists, computer hardware and software designers, and electrical engineers.”[8]

Keeping data in Germany will not keep the NSA's legion of cyber-warriors out. Indeed, rather than focusing on *where* the data is kept, you should be focusing your attention on the need to encrypt data, so that when hackers do compromise German servers or gain access to internal German telecommunications networks, the only data they can steal is encrypted, and thus far less useful to them. Rather than focusing on the “German cloud”, you should instead be investing resources into the rapidly advancing field of “cloud cryptography”,[9] which permits you to put data in the cloud, without worrying about where it is stored, or which governments might be able to compel a service provider into turning it over.

Merkel-gate **and German law enforcement surveillance of telephones**

In October 2013, Der Spiegel revealed that the NSA had been spying on the telephone communications of German Chancellor Angela Merkel.[10] Subsequent news reports revealed that NSA's secretive Special Source Operations (SSO) division had installed electronic surveillance equipment in a “spy nest” on the roof of the American Embassy in Berlin.[11] Although German politicians were outraged to learn that the

[6] *See* Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm, Spiegel Online, September 20, 2013, http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

[7] *See* Laura Poitras, Marcel Rosenbach and Holger Stark, 'A' for Angela: GCHQ and NSA Targeted Private German Companies and Merkel, Spiegel Online, March 29, 2014, http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html.

[8] *See* Matthew Aid, Inside the NSA's Ultra-Secret China Hacking Group, Foreign Policy, June 10, 2013, http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group.

[9] *See* Richard Falkenrath and Paul Rosenzweig, Op-Ed: Encryption, Not Restriction, Is The Key To Safe Cloud Computing, NextGov, October 5, 2012, http://www.nextgov.com/cloud-computing/2012/10/op-ed-encryption-not-restriction-key-safe-cloud-computing/58608/.

[10] *See* Jacob Appelbaum, Holger Stark, Marcel Rosenbach and Jörg Schindler, Berlin Complains: Did US Tap Chancellor Merkel's Mobile Phone?, Spiegel Online, October 23, 2013, http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html.

[11] Embassy Espionage: The NSA's Secret Spy Hub in Berlin, Spiegel Online, October 27, 2013, http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

Americans were spying on German telephone calls, this should not have come as a surprise.
The millions of mobile telephones used by Germans are not secure and are vulnerable to interception using widely available equipment. One of the first companies in the world to sell special-purpose surveillance devices designed to track mobile phones and intercept telephone calls was Rohde & Schwarz, a German company.[12] The IMSI catchers sold by this company since the mid-1990s exploit well known security flaws that are still present in the latest $600 smartphones sold to consumers in the United States and in Germany.

IMSI catchers are used by law enforcement agencies in Germany and their use is authorized by statute,[13] which also mandates annual statistical reports describing their use be published by the Parliament.[14] There have been several formal parliamentary questions submitted regarding the use of IMSI catchers,[15] as well as a decision from the German Constitutional Court permitting their use.[16] It therefore cannot be said that IMSI catchers, or the fact that mobile telephones in Germany can be spied upon with special equipment, are a big secret. The only surprise, it is seems, is that the American government is using the same (or similar) surveillance equipment that the German police regularly use to monitor German citizens, and are using it to spy on your political leaders.

Each year, at the Chaos Computer Club Congress, some of the best security researchers in the world (many of whom are German) demonstrate serious security flaws in mobile telephone networks.[17] Each year, the cost of interception goes down,[18] yet governments, including Germany's, do nothing to make sure their citizens' telephone calls are secure.

The problem, of course, is that real telephone security, provided through “end-to-end” encryption technology, would make police wiretaps difficult, if not impossible. To effectively protect the phone calls of Germans from American, Russian, Chinese and Israeli surveillance, you would have to require that German phone networks upgrade to secure communications technologies that your own law enforcement agencies would also not be able to monitor. This would no doubt be unpopular with the German law enforcement community, but also perhaps many German voters, once they learned that terrorists, drug dealers and pedophiles could no longer be wiretapped or covertly tracked by the authorities.

There is no communications technology that exists that will keep out a sophisticated foreign intelligence agency, while still permitting “lawful access” by domestic law enforcement. If anything, lawful surveillance systems built into communications networks are an irresistible target for foreign intelligence agencies.[19] Once you accept that, then the real problem becomes political, not technical: Do

[12] The earliest public document describing IMSI catchers and the Rohde & Schwarz products is an article in 1997 by Dirk Fox, a German security consultant. See Dirk Fox, IMSI-Catcher, Datenschutz und Datensicherheit, 21:539–539, 1997, available at http://www.secorvo.de/publikationen/imsi-catcher-fox-1997.pdf. Five years later, Fox published an updated, more in-depth article about the same technology. See Der IMSI-Catcher, Datenschutz und Datensicherheit, 26:212–215, 2002, http://www.secorvo.de/publikationen/imsicatcher-fox-2002.pdf.

[13] *See* Section 9 of the Federal Constitution Protection Act (Special Forms of Data Collection), paragraph 4, http://www.gesetze-im-internet.de/bverfschg/__9.html.

[14] *See* http://dip21.bundestag.de/dip21/btd/17/127/1712774.pdf (2011 data).

[15] *See* http://dip21.bundestag.de/dip21/btd/14/068/1406885.pdf and http://dipbt.bundestag.de/dip21/btd/17/076/1707652.pdf.

[16] *See* http://www.bundesverfassungsgericht.de/entscheidungen/rk20060822_2bvr134503.html.

[17] *See* Karsten Nohl and Chris Paget, GSM — SRSLY ?, 26th Chaos Communication Congress (26C3), December 27, 2009, http://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf.

[18] *See* Jon Borland, $15 phone, 3 minutes all that's needed to eavesdrop on GSM call, Ars Technica, December 29, 2010, http://arstechnica.com/gadgets/2010/12/15-phone-3-minutes-all-thats-needed-to-eavesdrop-on-gsm-call/.

[19] See Vassilis Prevelakis and Diomidis Spinellis, The Athens Affair, IEEE Spectrum, June 29, 2007,

you build your national communications to be secure, or to enable surveillance – knowing that surveillance will be possible by your own police, as well as several foreign intelligence agencies?

To date, Germany has prioritized surveillance-friendly communications networks. Perhaps that will change, but only if politicians are ready to accept that in order to keep the NSA out, the security technologies required will also necessarily prevent law enforcement agencies from conducting wiretaps and tracking legitimate targets.

A Regulatory Failure?

In December of 2013, Deutsche Telekom announced that it was the first German cellular telephone network operator to upgrade its network to deploy a more secure encryption algorithm ("A5/3") for voice communications over its cellular phone network.[20] This announcement was several months after the first Snowden disclosures, as well as the reports by Der Spiegel that Chancellor Merkel's phone calls were being monitored by the NSA.

Prior to the announcement, Deutsche Telekom, like most other wireless network operators, was likely using the A5/1 encryption algorithm. This algorithm, which was designed in the 1980s (and, weakened at the behest of several intelligence services),[21] was broken by researchers in the late 1990s,[22] but is still the most widely used cellular encryption algorithm in the world. Today, several surveillance companies (including firms in Germany[23]) sell sophisticated interception equipment capable of breaking this encryption algorithm and deciphering mobile conversations, in real-time.[24]

The A5/1 algorithm was broken by researchers in 1999, and in 2013, Deutsche Telekom finally upgraded their network to move from the weak A5/1 to the more secure A5/3. Why did it take 14 years and the largest surveillance scandal in decades for the customers of Germany's largest mobile operator to be upgraded to a more secure encryption algorithm?

I do not know the answer to this question, but I suggest that you ask your national telecommunications regulator, and see what, if anything, they have done to force German mobile network operators to promptly upgrade their networks and the phones used by their customers when they learn that a particular algorithm or cellular technology is insecure.

If, today, the phone calls of German journalists, business executives, and politicians can be intercepted with widely available equipment that can be purchased for just a few thousand euros, it suggests that

http://spectrum.ieee.org/telecom/security/the-athens-affair.

[20] *See* Deutsche Telekom upgrades wiretapping protection in mobile communications, December 9, 2013, http://www.telekom.com/media/company/210108.

[21] *See* Arild Færaas, Sources: We were pressured to weaken the mobile security in the 80's, Aftenposten, January 9, 2014, http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html (interviewing several experts involved with the creation of the original GSM A5/1 standard who claim the it was intentionally weakened as a result of pressure from the British government).

[22] *See* Alex Biryukov and Adi Shamir, Real Time Cryptanalysis of the Alleged A5/1 on a PC (preliminary draft), December 9, 1999. Final paper published as Alex Biryukov, Adi Shamir and David Wagner, Real Time Cryptanalysis of A5/1 on a PC, Fast Software Encryption, Lecture Notes in Computer Science Volume 1978, 2001, pp 1-18. See http://cryptome.org/a51-bsw.htm.

[23] See Passive GSM Monitoring System for A5.1, A 5.2 (A5.0) Encryption, http://www.pki-electronic.com/products/interception-and-monitoring-systems/passive-gsm-monitoring-system-for-a5-1-a-5-2-a5-0-encryption/

[24] See Verint Sales Brouchure, 2013, http://s3.documentcloud.org/documents/885760/1278-verint-product-list-engage-gi2-engage-pi2.pdf.

your telecommunications regulator is not doing as much as they should to protect the security of Germany's telephone networks.

The role of technical experts in the surveillance oversight process

Surveillance is now, more than ever before, a highly-technical subject, the finer details of which can be difficult for political scientists and lawyers to understand. It is therefore vital that your committee, as well as every agency and committee with a role in the surveillance oversight process in Germany be assisted by technical experts, who can explain these deeply technical concepts to those making the decisions and writing the reports.

At the ACLU, I am embedded within a team of lawyers, who work on our surveillance related litigation. My primary job is to explain the technology to them, to make sure they understand the technical details related to the cases they are working on, and to ensure that the arguments we make in court are technically accurate. Prior to joining the ACLU, I worked for the Federal Trade Commission, the primary regulator of privacy in the United States Government, in a similar role.

I was the first technologist hired by the FTC and the ACLU. At both organizations, hiring technologists has changed the way they do business, and enabled them to make arguments that are far more technically sophisticated than they would have been able to do so before. After I left the FTC, the agency hired several more technologists, and even created a Chief Technologist position. Similarly, the ACLU this year hired a second full-time technologist. Technologists are a force-multiplier, enabling teams of lawyers to be far more effective at their jobs.

Inviting technical experts to testify before your committee is a great start. However, this is not enough. I urge you to hire technical advisors, and to ensure that the committees and courts that oversee your own national surveillance apparatus also have the technical expertise to really understand what is being done.

Thank you,

Christopher Soghoian
csoghoian@aclu.org