Testimony of Dr. Christopher SOGHOIAN
Principal Technologist
Speech, Privacy, and Technology Project
American Civil Liberties Union

Before the LIBE Committee Inquiry on Electronic
Mass Surveillance of EU Citizens

18 December 2013

Members of the LIBE committee, thank you for the invitation to testify before you today, and thank you for seeking out the advice of technical experts. In my testimony before you today, I will make two main points.

First, that the mobile telephone networks in Europe are not safe – from the American intelligence agencies, from the Russians, the Chinese and other governments too.

Second, that European policy makers and regulators have had ample warning about serious security flaws that expose European citizens' communications to interception. Sadly, these warnings have often been ignored, or worse, instead of fixing the flaws, they have been exploited by European law enforcement and intelligence agencies.

The security of mobile networks

In October of this year, the topic of mobile phone privacy instantly became an issue of significant political concern after journalists writing for Der Spiegel revealed that the US National Security Agency (NSA) had for years monitored the mobile telephone calls of German Chancellor Angela Merkel.[1] Subsequent reporting also revealed that the phone spying was conducted by a joint NSA/CIA unit, which operates out of 80 US embassies and consulates.[2]

Ordinarily, it should not matter that mobile phone signals can be intercepted as they pass through the air. The security of the mobile telephone network should not depend upon the difficulty of recording the signals, but rather, there should be other security technologies in use that protect our calls.

For example, we all regularly use open WiFi networks at coffee shops and hotels to conduct sensitive tasks such as sending emails and online banking. Although these WiFi networks are not secure, the Internet services we use over the WiFi networks are themselves secure. The "lock icon" you see in your web browser when you login to your bank's website, to Google or Facebook is an indication that your interactions with those sites are secure, even if the WiFi network you are using is not.

---

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

[2] *See* SPIEGEL Staff, Embassy Espionage: The NSA's Secret Spy Hub in Berlin, Der Spiegel, October 27, 2013, *available at* http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html. The Der Spiegel story originally included a slide showing all of the Special Collection Service locations, but this was subsequently replaced with a redacted version. An archive of the original unredacted slide is *available at* http://cryptome.org/2013/10/cia-nsa-scs-map.jpg.

Sadly, there is no "lock icon" built into our mobile phones. The security that is built into mobile telephone networks is decades old, very weak, and in fact, quite thoroughly broken. As such, there is little protecting our calls from the NSA, or in fact, any other government.

European governments use mobile phone interception technology

The security vulnerabilities in "GSM" mobile telephone networks exploited by the NSA have been known in Europe for nearly two decades. For example, Rohde & Schwarz, a German company, is generally believed in 1997 to have created the first commercial device capable of intercepting mobile telephone calls.[3] Several other European companies, including firms in Germany, Switzerland and the United Kingdom manufacture and sell similar surveillance products that are capable of exploiting long-standing security flaws in mobile telephone networks to intercept calls and monitor nearby phones.[4]

The customers of these surveillance companies include law enforcement and intelligence agencies in several European countries. Although this technology is generally introduced and used in secret, in Germany, it has been used and regulated in a relatively transparent manner. For example, German law regulates the use of this technology by government agencies,[5] and requires statistical reports be published each year.[6] Moreover, it has been the subject of several formal parliamentary questions,[7] as well as a decision from the German Constitutional Court permitting their use.[8]

This of course means that your own law enforcement and intelligence agencies know that telephone networks in your respective countries can be spied on by anyone with the right equipment. They know this, because they have purchased and are using this equipment for surveillance. Furthermore, as

---

[3] 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 (in German). 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 (also in German).

[4] See *MMI Research Ltd v Cellxion Ltd & Ors* [2009] EWHC 418 (Pat) (11 March 2009) available at http://www.bailii.org/ew/cases/EWHC/Patents/2009/418.html (describing the demonstration of the GSM-X interception device to potential government clients in 1999 by MMI Research Ltd, a British surveillance equipment manufacturer). *See also* http://www.neosoft.ch/.

[5] *See* Section 9 of the Federal Constitution Protection Act (Special Forms of Data Collection): http://www.gesetze-im-internet.de/bverfschg/__9.html, paragraph 4. See generally Chapter on German interception law by Rau in http://books.google.com/books?id=GNCpeUdVkOoC&lpg=PA654&pg=PA349#v=snippet&q=IMSI&f=false

[6] http://dip21.bundestag.de/dip21/btd/17/127/1712774.pdf (2011 data), http://dipbt.bundestag.de/dip21/btd/17/086/1708638.pdf (2010 data)

[7] http://dip21.bundestag.de/dip21/btd/14/068/1406885.pdf (2001) http://dipbt.bundestag.de/dip21/btd/17/076/1707652.pdf (2011)

[8] See http://www.akvorrat.at/sites/default/files/VDS_Materialien/Art%2029%20WP%2010th_annual_report_en.pdf (An English language summary of the ruling by the Federal Constitutional Court on 22 August 2006 on the use of the IMSI-catchers in criminal proceedings. See also http://www.bundesverfassungsgericht.de/entscheidungen/rk20060822_2bvr134503.html (the decision of the court, in German)

European companies are manufacturing and then exporting this technology outside your own borders, it is likely that other government agencies, such as national telecommunications regulators and export permit granting agencies, also know about the long-standing telephone network security flaws, and the technologies that can exploit them.

The globalization of surveillance

It would be one thing if this technology were only manufactured by European companies and sold to European governments. However, that is not the case. Companies in the United States, China, Russia, India and Israel sell similar technology, to their own governments, and to other governments as part of the five billion dollar global market for commercial surveillance technology.[9] Mobile telephone interception devices are reportedly among the "bestselling items" exhibited at surveillance industry trade shows.[10]

Indeed, a few weeks after it was revealed that the United States was spying on the telephone calls of Chancellor Merkel, media reports revealed that China, Russia, The United Kingdom and North Korea were also intercepting her calls too.[11] Even if the American government keeps its promise to stop spying on the calls of Chancellor Merkel, no amount of political pressure will stop these and other governments from using their spying equipment. If the telephone can be intercepted, they will be intercepted those governments capable of doing so. If you don't want your calls to be intercepted, this means you must do something about it.

Clear warnings

During the past few years, prominent security researchers have repeatedly warned about the flaws in mobile telephone networks that these "government-grade" surveillance devices exploit. Although interception once required a $50,000 commercial surveillance device to intercept calls, it is now possible for researchers, hobbyists, and hackers to build their own interception devices for a few hundred dollars. For example, in 2010, a security researcher intercepted calls from the phones of audience

---

[9] *See* Nicole Perlroth, Software Meant to Fight Crime Is Used to Spy on Dissidents, New York Times, August 30, 2012, *available at* http://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html ("The market for such technologies has grown to $5 billion a year from 'nothing 10 years ago,' said Jerry Lucas, president of TeleStrategies, the company behind ISS World, an annual surveillance show.")

[10] *See* Stefan Krempl, 28C3: New attacks on GSM mobiles and security measures shown, The H Open, December 28, 2011, available at http://www.h-online.com/open/news/item/28C3-New-attacks-on-GSM-mobiles-and-security-measures-shown-1401668.html ("Following a trip earlier this year to the Mecca of the "cyber-industrial complex", the Intelligent Support Systems (ISS) trade fair which is held at various sites in Asia and the Middle East, Nohl reports that the bestselling items in the espionage community at present are devices for monitoring mobile phones, such as IMSI catchers.")

[11] *See* Merkel's phone tapped by at least 5 countries, MarketWatch, November 25, 2013, *available at* http://www.marketwatch.com/story/merkels-phone-tapped-by-at-least-5-countries-2013-11-24

members at the DEF CON security conference in Las Vegas.[12] Mobile telephone interception technology has been democratized.[13]

In spite of the repeated warnings by researchers, telecommunications regulators in Europe (and in my own country) have ignored the security problems. Likewise, the major telephone service providers have neither been forced to improve the security of their networks nor warn their customers about the risks.

As you continue your inquiry, I strongly encourage you to look into the widespread failure of European telecommunications regulators to protect your telephone networks against the threat of interception by governments using technologies that are now widely available. It should not have taken the leaks by Edward Snowden to get policy makers to start thinking about the security of your telephone networks.

Securing your communications networks

If you do not wish for the Americans, the Russians, the Chinese or any other foreign government to spy on the phone calls of your policy makers, business leaders and journalists, you must take action. However, protecting your telephone networks from such surveillance threats will also require the large-scale deployment of advanced encryption technologies that will thwart your own law enforcement and intelligence agencies' use of the same interception technology.

Your senior political leaders likely already have government-issued encrypted telephones, although, I suspect, few, if any members of this committee have them. These devices are usually quite expensive, although communications security does not have to be a luxury. In fact, freely available open-source encrypted voice communication software apps already exist, which anyone can download and use today.

The real question, is whether you are ready to promote, or, better, to provide all of your citizens with the same degree of communications confidentiality (and thus protection from wiretapping, by governments foreign and domestic) that your own political leaders already enjoy. I strongly urge you to take action to protect the communications of all Europeans, through the use of privacy enhancing technology.

Thank you.

---

[12] *See* Chris Paget, Practical Cellphone Spying, Defcon 18, July 31, 2010, video at 23:36, available at http://www.youtube.com/watch?v=DU8hg4FTm0g.

[13] *See* Ralf-Philipp Weinmann, Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf, 6th USENIX Workshop on Offensive Technologies, August 6, 2012, available at ("In the past, spoofing a GSM network required a significant investment, which limited the set of possible attackers. . . Open-source solutions such as OpenBTS allow anyone to run their own GSM network at a fraction of the cost of carrier-grade equipment, using a simple and cheap software-defined radio. This development has made GSM security explorations possible for a significantly larger set of security researchers.")