One Year After Snowden: How Safe Are Your Calls and Emails?

By Christopher B. Hopkins

On June 5, 2013, the world learned of Edward Snowden in a ground-breaking news story, "NSA Collecting Phone Records of Millions of Verizon Customers Daily." Over this past year, we have learned a little more about Snowden himself and considerable more about the NSA's mass surveillance methods. Articles in *The Guardian* and *Washington Post* have come out nearly every week, like Saturday serial moves from the 1950's, and it has been easy to lose touch with the unraveling story of how modern spy technology spans beyond what was once considered science fiction. This article provides an overview of the Snowden revelations and outlines some considerations for securing your calls and emails.

Before Snowden, there were some warning signs that, after September 11, the government was pursuing phone and email data on a massive scale without warrants. The Foreign Intelligence Surveillance Act of 1978 (FISA), which had been relatively unchanged prior to September 11, was modified in 2001, 2007, and 2008 to the point that probable cause and specific information were no longer required for mass surveillance. Along the way, in December 2005, the New York Times reported, "Bush Lets U.S. Spy on Callers Without Courts." On the other hand, in February 2013, the U.S. Supreme Court declined to permit *Clapper v. Amnesty International et al.* proceed with its claim about government spying -- in the pre-Snowden era, there was insufficient data that reporters and activists, much less the general public, were subject to having telephony data inspected. *Clapper* gained little sustained attention in the media and was still largely forgotten, four months later, when the first Snowden disclosure was published.

What Have We Learned About Phone & Internet Surveillance Since June 2013?

- *Telephony Metadata*: all call detail records, from local to international, are collected.
- *PRISM*: a mass surveillance system collects data from the major internet companies such as AOL, Apple, Facebook, Google, Microsoft, Skype, and Yahoo (*Washington Post* claimed that, "from inside a company's data stream, the NSA is capable of pulling out anything it likes…").
- *$278 Million Dollar Budget in 2013*: the government paid "reasonable reimbursement" expenses to internet companies.
- *EvilOlive*: a massive filter collects and analyzes internet metadata in bulk.
- *Upstream*: a disclosed Powerpoint slide reveals that the NSA has fiber optic taps at various points among the continents.
- *Even the FISC judges were surprised*: the court which approves requests in secret did not have a full appreciation for the scope of mass surveillance. In one opinion which the NSA published in light of the Snowden disclosures, the judge wrote, "that revelation [of Upstream capturing internet data] fundamentally alters the Court's understanding of the scope of the collection conducted… and requires careful reexamination of many of the assessments and presumptions underlying its prior approvals."
- *The government was not always fully transparent with FISC*: one judge wrote, "the Court is troubled that the government's revelations regarding NSA's acquisition of internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."
- *XKeyscore*: using this program, analysts can search emails, chats, browsing history and more by a person's name, phone number, IP address, keywords, sites visited, etc. Snowden disclosed the "unofficial XKeyscore Users Guide" which shows how an analyst can search all emails to/from person's email address or, conversely, can determine who accessed a specific webpage.
- *Facebook, Twitter, and More:* the title of a September 2013 *New York Times* article revealed, "NSA Gathers Data on Social Connections of U.S. Citizens."
- *NSA Collects Contact Lists*: the agency reportedly amasses 250 million email views and contact lists of users every year.
- *NSA Can Beat Most Safeguards*: in September 2013, it was reported that the NSA has "circumvented or cracked" most of the encryption used for banking, trade secrets, and medical records.
- *Encryption May be Compromised*: In late 2013, RSA Security issued an advisory to stop using one of its encryption key generators (you may have such a key-fob code generator for remote access to your firm's email). In June 2014, True Crypt admitted that it "may contain unfixed security issues."
- *NSA Can Hack All of the Major Smartphones*: reported by *Der Spiegel* in the Fall of 2013 and confirmed in the May 2014 NBC Snowden interview.
- *Unknown?*: Snowden reportedly has excerpts from NSA Powerpoints which no news agency will publish.

What Are the Best Practices for Secure Phone Calls and Internet Use?

- *Endpoint Security*: you are weakest where you enter and leave the internet, particularly wireless and mobile devices.
- *ABA's Comment*: the American Bar Association amended a comment to the Model Rules that, in our ethical requirement to stay abreast of technology, consider the "benefits and risks associated with relevant technology."
- *Questions to Ask*: How sensitive is the data? What is the harm of disclosure? What is the cost of additional safeguards? Are they workable?
- *There is no expectation of privacy in international calls* -- the U.S. does not need a warrant and you can presume other countries are likewise monitoring.
- *Government and Commercial Monitoring*: when possible, use Tor for sensitive internet research and perform basic queries on non-tracking sites like DuckDuckGo, Privatelee, and Startpage.

Christopher B. Hopkins is a partner in the West Palm Beach office of Akerman LLP. He accepts secret handshakes, carrier pigeons, and smoke signals but prefers the less secure email to christopher.hopkins@akerman.com.