What NSA Surveillance Means to Law Firms

by Sharon D. Nelson, Esq. and John W. Simek

Of Heroes and Villains

The Chinese are the villains, engaged in a pervasive course of state-sponsored cyberattacks. Unless you've been living the life of a hermit, you've heard that a lot in the course of the last year.

But now we've learned that the cybersecurity of law firms is at risk from a newly discovered source – The National Security Agency. After 9/11, many Americans embraced the Patriot Act, numb from the tragedy and justifiably concerned about terrorist plots on American soil. After a time, most folks became complacent and more or less bought the government's reassurance that federal surveillance involved primarily foreigners and that it was not snooping on the activities of ordinary Americans.

That proved wrong in a big way. Courtesy of Edward Snowden (like him or hate him, he exposed a lot of illegal and unconstitutional activities), we have learned that we are closer to the "Big Brother" state of George Orwell's "1984" than we ever thought possible. So let's take a look at what we now know and then we'll turn to the implications for lawyers.

The NSA's Bag of Tricks – and its Targets

We got up as we wrote this to news that the NSA had hacked into the video conferencing system of the United Nations and was listening in on various colleagues, reputedly focusing in on the European Union. Terrific, that ought to shore up our strained relations with our European allies.

Thanks again to Edward Snowden, *The Washington Post* published a story based on an internal National Security Agency (NSA) audit and other top secret documents. The story indicates that the NSA has broken privacy rules or overstepped its legal authority thousands of times each year since it was granted broad new powers in 2008.

Most of the violations involved unauthorized surveillance of Americans or foreign intelligence agents in the U.S., surveillance that is restricted under statute and Executive Order. They resulted in the interception of U.S. e-mails and telephone calls.

How do they do that? Recent reports have indicated that the NSA is even intercepting shipments of computers purchased online in order to infect them with spyware or replace components with its own malware-installed hardware. That's pretty gutsy. Of course you need to be specifically targeted by the NSA before you'll get a little "something extra" arriving along with the shiny new computer.

Suppose you didn't order a new computer. How could the NSA intercept your data? Additional revelations were disclosed at the recent Chaos Communications Congress. Apparently, there is a whole catalog of equipment and software that the NSA is willing to sell to other agencies. One such device is called the NIGHTSTAND. It is designed to hack WiFi devices from eight miles away. It is a standalone tool and can exploit targets including Win2K, WinXP, WinXP SP1 and Win XP SP2 systems running Internet

Explorer version 5.0-6.0. There is no report that they have hardware for the more modern operating systems or browsers. Yet another reason to make sure you are up to date with patches and versions.

What is XKeyscore?

Again by way of a Snowden leak, *The Guardian* revealed new details on a very powerful, secret program run by the U.S. government called XKeyscore. With the program, NSA employees can obtain everything from phone numbers to e-mail addresses. The NSA can also see e-mail content, Internet activity, browser history, and an IP address. According to the files and to Snowden, no warrant is needed.

Has the NSA been using this capability on U.S. citizens? With the information currently available, we're not sure. If there is any cold, cold comfort in the new revelations, it is that the sheer volume of data means that content is only available for 3-5 days and metadata for 30 days. Each day, 1 to 2 billion records are added, necessitating deleting or transferring data. To solve that problem, it appears that the NSA has created other databases where "interesting" information can be stored for later analysis.

Microsoft Helps the NSA View Its Encrypted Data

According to yet another article from *The Guardian,* citing top secret documents from you-know-who, Microsoft has:

- Helped the NSA circumvent its encryption so that the agency can intercept web chats on the Outlook.com portal
- Given pre-encryption stage access to e-mail on Outlook.com, including Hotmail
- Allowed the NSA easier access to SkyDrive
- Helped to triple the amount of Skype video calls being collected through Prism

FISA Court Becoming a Parallel Supreme Court

The Foreign Intelligence Surveillance Act (FISA) created the Foreign Intelligence Surveillance Court (FISC) often referred to as the FISA Court. Commentators have said it is now almost a parallel Supreme Court. They are particularly troubled by a recent decision of the Court creating a “special needs” doctrine.

The special needs doctrine was established in 1989 by the Supreme Court in a ruling allowing the drug testing of railway workers, finding that a minimal intrusion on privacy was justified by the government’s need to combat an overriding public danger. The FISC judges have expanded that doctrine by ruling that the NSA’s collection and examination of Americans’ communications data to track possible terrorists does not run afoul of the Fourth Amendment. A once narrow doctrine is now very broadly used to collect communications.

It appears that a central concept of recent decisions is that collecting "metadata" - the times of phone calls, numbers dialed, length of call etc. - is fine if the government establishes a valid reason under national security regulations. Content is protected. As one official said, “The basic idea is that it’s O.K. to create this huge pond of data but you have to establish a reason to stick your pole in the water and start fishing.” We’re not even sure we believe that official – our mental image is of a dragnet being pulled through many bodies of water.

To close with one of the most disquieting facts recently revealed, the NSA can now reach roughly 75% of all Internet traffic in the U.S. And while the NSA's purported mission is to target foreigners, the NSA sometimes retains the written content of e-mails sent between citizens with the U.S. How often is sometimes? We don't know and don't believe there is any reliable answer to the question. But it disturbs us even more that the U.S. has almost completed construction of a datacenter in Utah that would, some reports say, hold 5 years of the communications of U.S. citizens. Of course, that's not what the government says it will be doing with this top-secret datacenter. "Trust Me, I'm From the Government?" That just isn't working out lately folks. Reassuring words from the President notwithstanding, the process has not been at ALL transparent. And it took a whistleblower to learn the truth.

Even the ABA, at its August meeting of the House of Delegates, passed a cybersecurity resolution. The original resolution only talked about stopping intrusions into lawyers' networks by foreign governments - it was changed to simply "governments" in light of our new knowledge of what our own government is doing.

Quantum Computers

Edward Snowden has released additional documents revealing NSA's effort to build "a cryptologically useful quantum computer" as part of a $79.7 million research program. Quantum computers have long been a goal of many in the scientific community. If the NSA is successful in building a quantum computer, all current forms of public key encryption would be broken. The common belief is that the NSA is no further along with their quantum computer development than anybody else in the world. We're probably safe for the time being.

Soooo - How is a Law Firm to Keep its Data Confidential?

The NSA revelations have serious implications for lawyers. We used to tell lawyers that Skype was secure – but then Microsoft bought it and began changing the network architecture by running the calls through its servers – and now, apparently, unlocking data for the NSA from time to time. And what about the lawyers who are storing their data in SkyDrive? Or the solos who are using Hotmail?

Frankly, the NSA revelations have given us a lot of pause. It is one thing to protect against foreign governments who have to perform cyberattacks to get your data and quite another to protect against your own government when it is given the keys to your data. How can you be ethically compliant in light of the potential threat from our own government?

Battening Down the Hatches

Cloud Computing

Roughly half of all law firms are now holding at least some data in the cloud. The recent news has shaken them, as well it should. But we are not preaching a mass exodus from the cloud. Two major points here:

- If you are fundamentally storing all your data in a datacenter, your biggest problem is whether the datacenter personnel can gain access to your data. For this reason, we do not recommend putting law firm data on servers owned by the datacenter. It doesn't matter whether there is a master decryption key or whether a "back door" is built in. The safest way to store data in a datacenter is to use a hybrid solution – where you own the equipment and the access to your equipment and data is restricted to yourself and your own IT folks in locked racks. Any emergency access to the data, by contract, should require immediate reporting to you and, again by contract, you should receive notice of any law enforcement request for the data right away so you can file a motion to quash. Major players in the market may not give you these terms but the smaller ones will. One caveat: If a request is made under The Patriot Act, you're toast – your data will be handed over on a silver platter. But the vast majority of law enforcement requests are not made pursuant to the Patriot Act.

- If you are using specific clouds to store data, encrypt your data before sending it. A great example is Dropbox, now utilized by so many litigators. If you encrypt your Word or PDF documents before putting them in Dropbox, it doesn't matter that Dropbox holds a master decryption key (and it does). Even if it attempts to decrypt for the federal agents at the door, Dropbox can only provide them with garbage. What the feds can do with the data is apparently changing. News reports indicate increasing success in breaking encryption, but we have yet to see proof. And yes, encryption will work for SkyDrive, the iCloud (depending on the data type and device used), etc. And no, this is not hard. Stop being afraid of the word encryption. If you password protect a Word or PDF document (which you can do natively within the program – just search "Help"), it is encrypted. Just promise us you won't send it as an attachment with the decrypt key in the text of the e-mail.

Encryption

You should also be taking a hard look at encryption on your smartphones – iPhones are encrypted when configured with their PINs, poorly with a 4 digit pin – you need a complex password. BlackBerrys are natively encrypted when "Content Protection" is enabled. Android encryption must be turned on in Settings, but it is there.

No lawyer should be performing work on a personal machine. In today's world, every lawyer should be issued a firm laptop and smartphone so that security can be controlled and monitored. This means no BYOD unless you are prepared to implement a MDM (Mobile Device Manager) solution to the tune of several thousands of dollars. All laptops, like smartphones, should have whole disk encryption.

Bottom line…you should be encrypting data on all devices. The one disclaimer is the recent news concerning the capabilities of the NSA. As noted security commentator, Bruce Schneier, has stated, "The NSA is breaking most encryption on the Internet." This is accomplished by intercepting the data and compromising the secure certificate provider infrastructure or using intentional weaknesses inserted in encryption products. As an example, RSA Security released an advisory to stop using the Dual Elliptic Curve Deterministic Random Bit Generation (Dual EC DRBG) because of weaknesses in the algorithm.

Apparently, the NSA had their fingers in the design of Dual EC DRBG. Some have even suggested using encryption and security products from vendors that are not based in the United States to minimize any potential NSA back doors. The good news is that a large number of products do not use the flawed Dual EC DRBG.

Should You Move Your Data Out of the Country?

Trust us, this is being done. But our answer, for the moment, is no. First, having data in foreign countries means you are subject to their laws – and cross-border data privacy issues are a nightmare. Second, don't assume that NSA hasn't gotten its hooks into foreign carriers. There has been a lot of evidence suggesting that it has. Personally, we would rather shore up our defenses at home. There are companies in the U.S. pledging that they will not cooperate with the government and lots of new customers for those companies.

Passwords

The government has already displayed an appetite for hacking. Don't make it easy for them. Have strong passwords that are regularly changed. Enforce your password policies. Make sure passwords are not being shared – still a lamentably common practice.

Security audits

We used to say that you needed security audits every 6-12 months to keep the Chinese and the cybercriminals out of your networks. Now we add that you need to protect your networks against our own government – sad but true. By in large, big firms will go to big companies to perform these audits. Solos and small will head to smaller firms where the price tag isn't so high. Get a referral from trusted friends, check out credentials, etc. – but don't fail to do these audits.

Training

We can never say it often enough. Human beings are the greatest security threat. Train them – over and over again – and remember that things change very quickly in the information security world. Even in a small firm, there should at least be annual training sessions by someone well-versed in information security.

Parting Words

Lest we seem overly paranoid, we'll give the parting words to George Washington – who better than the father of our country?

"Government is not reason; it is not eloquent; it is force. Like fire, it is a dangerous servant and a fearful master."

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com