Edward Snowden: How Will NSA Revelations Change the Profession of Law?

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

Perfectly normal people grow slight lunatic when talking about Edward Snowden. Cries of treason were loud at the beginning. As time and revelations of NSA surveillance went on, more and more people used the word whistleblower rather than traitor. In December, the NSA itself talked about amnesty for Snowden – nixed by the federal government, at least for now. He cannot do what so many want – give the documents back. Clearly, they are in the hands of journalists across the globe. Recent revelations have shaken lawyers, especially at large and global firms and it is clear we too will have to live in what one journalist called the "post-Snowden era." So let's get to know him.

Who is Edward Snowden?

He was born on June 21, 1983. He was described by friends and neighbors as being shy, quiet and nice. His father called him a deep thinker. He was fascinated by Japanese culture and, as a young adult, listed Buddhism on a military recruitment form. He once told the *Washington Post* that he was an ascetic, rarely left home and had few needs.

Without going into too much detail, he joined the Central Intelligence Agency in 2006 as a systems administrator and telecommunications systems officer. In 2007, the CIA stationed him with diplomatic cover in Geneva, where he was responsible for network security.

He resigned from the CIA in February 2009 and went to work for Dell and was stationed in an NSA facility in Japan. He remained with Dell until early 2013. He was one of approximately 1000 NSA system administrators allowed to look at many parts of the network without leaving an electronic trail and succeeded in getting flash drives into a secure environment. He held a position with the NSA for

twelve months before moving to private contractor Booz Allen Hamilton for less than three months, working at an NSA facility in Hawaii.

Snowden has said he took a pay cut to work with Booz Allen so he could gather data about global NSA surveillance and leak it. According to Booz Allen, Snowden's employment was terminated on June 10, 2013, "for violations of the firm's code of ethics and firm policy."

A former NSA co-worker told *Forbes* that although the NSA was full of smart people, Edward Snowden was "a genius among geniuses." He was described as a "principled and ultra-competent, if somewhat eccentric employee, and one who earned the access used to pull off his leak by impressing superiors with sheer talent." Snowden created a backup system for the NSA that was implemented, and often pointed out security bugs to the agency. The former colleague said Snowden was "given full administrator privileges, with virtually unlimited access to NSA data" because he could "do things nobody else could." Snowden had been offered a position on the NSA's elite staff of hackers, Tailored Access Operations (TAO), but turned it down for the contractor position at Booz Allen.

He kept a copy of the Constitution on his desk to cite when arguing against NSA activities he thought might violate it. He has said many times that he tried to get people in the NSA to recognize that many of its activities were illegal – and that many were indeed deeply concerned – but no one wanted to mount a charge against the agency.

Though several government officials have tried to say that his actions were directed by a foreign power, there is simply no evidence of that. His former colleague, while disagreeing with his methods, said "I understand why he did it. I won't call him a hero, but he's sure as hell no traitor."

What has he revealed thus far?

On May 20, 2013, Snowden flew to Hong Kong. He was there when the initial articles based on the leaked documents were published, beginning on June 5th. A continuing series of articles were distributed worldwide by, most notably, *The*

Guardian (Britain), *Der Spiegel* (Germany), *The Washington Post* and *The New York Times*. Here's what we now know:

- The first program to be revealed was PRISM which allows for a court-approved, front-door access to Americans' Google and Yahoo accounts.
- A report also revealed details of Tempora, a British black-ops surveillance program run by the NSA's British partner, GCHQ. The initial reports included details about NSA call database, Boundless Informant, and of a secret court order requiring Verizon to hand the NSA millions of Americans' phone records daily, the surveillance of French citizens' phone and Internet records, and those of "high-profile individuals from the world of business or politics.
- Next was XKeyscore, which allows for the collection of 'almost anything done on the internet', which was described by *The Guardian* as a program that "shed light" on one of Snowden's more contentious claims: "I, sitting at my desk [could] wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email."
- It was revealed that the NSA was harvesting millions of e-mails and instant messaging contact lists, searching email content, tracking and mapping the location of cell phones, undermining encryption via Bullrun and that the agency was using cookies to "piggyback" on the same tools used by Internet advertisers "to pinpoint targets for government hacking and to bolster surveillance." The NSA was shown to be "secretly" tapping into Yahoo and Google data centers to collect information from "hundreds of millions" of account holders worldwide by tapping undersea cables using the MUSCULAR program.
- Leaked documents showed NSA agents spied on their "love interests", a practice NSA employees termed LOVEINT. The NSA was also shown to be tracking the online sexual activity of people they termed "radicalizers", in order to discredit them.
- Snowden's disclosures created tension between the U.S. and some of its close allies revealing that the U.S. had spied on Brazil, France, Mexico, Britain, China, Germany and Spain, as well as 35 world leaders, most

notably German Chancellor Angela Merkel, who said "spying among friends" was "unacceptable" and compared the NSA with the Stasi.

- The NSA's top-secret "black budget", exposed the "successes and failures" of the 16 spy agencies comprising the US intelligence community, and revealed that the NSA was **paying** private American tech companies for "clandestine access" to their communications networks. The agencies were allotted $52 billion for the 2013 fiscal year.
- An NSA mission statement titled "Sigint Strategy 2012–2016" affirmed that the NSA plans for continued expansion of surveillance activities. Their stated goal was to "dramatically increase mastery of the global network" and "acquire the capabilities to gather intelligence on anyone, anytime, anywhere."
- The infamous NSA ANT catalog was revealed, which offers a remarkable number of products available to the NSA and others to perform surveillance activities.
- The NSA spies on Wikileaks and records information about its visitors.
- Apparently, most recently the NSA has received attorney-client communications from its counterpart in Australia.

How did he gather all the data?

In a couple of ways. He used easily available web crawler software to scrape data out of NSA's systems while he did his day job. Yes, much of it was automated. So this was a low tech, nearly amateur attack from the inside – and it is remarkable that there were not systems in place to detect it.

How many files did he access? Intelligence officials told the House of Representatives that he accessed 1.7 million files. These files include shared "wikis" to which intelligence analysis, operative and others contributed their knowledge.

Embarrassed NSA officials say that Snowden's activities would have been picked up if he had worked at the NSA headquarters in Fort Meade, MD, which was equipped with software designed to detect large volumes of data being accessed.

But the Hawaii facility had not yet been upgraded with modern security measures.

He was challenged a couple of times, but his explanations sounded rational in light of his duties backing up computer systems and moving information systems.

What Snowden really discovered was that while the NSA has huge electronic barriers to keep out foreign intruders, the protections it had against insiders were rudimentary. Officials have said that no one was looking "inside" the system in Hawaii for strange activity. Remarkable. And, apparently, it remains true that the NSA doesn't actually know what data Snowden possesses, a testament to some of the lousiest security we've seen anywhere.

What does all this mean for law firms?

The New York Times broke an amazing story on Saturday, February 15, 2014. The top-secret document demonstrated that an American law firm was monitored while representing a foreign government in trade disputes with the United States. The government of Indonesia had retained the law firm for help in trade talks, according to the February 2013 document. It reports that the NSA's Australian counterpart, the Australian Signals Directorate, notified the NSA that it was conducting surveillance of the talks, including communications between Indonesian officials and the American law firm, and offered to share the information.

The Australians told officials at an NSA liaison office in Canberra, Australia, that "information covered by attorney-client privilege may be included" in the intelligence gathering, according to the document, a monthly bulletin from the Canberra office. The law firm was not identified, but Mayer Brown, a Chicago-based global firm, was then advising the Indonesian government on several trade issues.

On behalf of the Australians, the liaison officials asked the NSA general counsel's office for guidance about the spying. The bulletin notes only that the counsel's office "provided clear guidance" and that the Australian agency "has been able to

continue to cover the talks, providing highly useful intelligence for interested US customers."

The NSA declined to answer questions about the reported surveillance, including whether information involving the American law firm was shared with United States trade officials or negotiators.

Note that this is not a story of tracking down terrorists. This is business espionage, pure and simple – something that Snowden has pointed out frequently.

In a statement to the Times, the NSA declined to comment on the details included in the Snowden document. Broadly speaking, the agency said, "Any allegation that the NSA relies on foreign partners to circumvent U.S. law is absolutely false. The National Security Agency does not ask its foreign partners to undertake any intelligence activity that the U.S. Government would be legally prohibited from undertaking itself."

Unfortunately, the credibility of the NSA is zilch. Our prediction is that law firms, in sensitive matters, may take an old world approach and dispatch lawyers to talk to clients in person - and not necessarily in a setting where surveillance might be expected.

Remember the old movie scenes of international spies talking to their informers in parks? What's old may well be new again.

Following news reports that a foreign ally of a U.S. intelligence agency may have spied on a BigLaw firm, the American Bar Association has asked the director of the National Security Agency and its general counsel for an explanation of how it deals with attorney-client privilege.

In a letter written on February 20th, ABA President James R. Silkenat asks the NSA's Director for an explanation of what policies and practices the NSA has in place to protect confidential information protected by the attorney-client privilege that may be received or intercepted—and whether those policies and practices were complied with in the alleged law firm incident. So far, there has been no response to Silkenat's inquiry.

For more than a year, we have told audiences that it was our assumption that the NSA (and perhaps others) were spying on U.S. law firms. Think about it. The U.S. government, mostly the FBI and the Secret Service, has been coming to law firms and advising them that they had been breached by foreign governments, hackers, etc. Audiences keep asking, "How did they know?"

We thought the only logical answer much of the time was that the NSA or one of its international counterparts in the Five Eyes alliance (United States, United Kingdom, Canada, Australia and New Zealand), had already infiltrated the law firms, and watched the other intruders come through the door.

Why did he do it?

In a December 2013 letter to the people of Brazil, Snowden wrote:

"There is a huge difference between legal programs, legitimate spying ... and these programs of dragnet mass surveillance that put entire populations under an all-seeing eye and save copies forever ... These programs were never about terrorism: they're about economic spying, social control, and diplomatic manipulation. They're about power."

Snowden's identity was made public by *The Guardian* at his request on June 9, 2013. He explained: "I have no intention of hiding who I am because I know I have done nothing wrong." He added that by revealing his identity he hoped to protect his colleagues from being subjected to a hunt to determine who had been responsible for the leaks. Snowden explained his actions saying: “I didn’t want to change society. I wanted to give society a chance to determine if it should change itself. All I wanted was for the public to be able to have a say in how they are governed.”

When Snowden met with representatives of human rights organizations, he said

“The 4th and 5th Amendments to the Constitution of my country, Article 12 of the Universal Declaration of Human Rights, and numerous statutes and treaties forbid such systems of massive, pervasive surveillance. While the U.S. Constitution marks these programs as illegal, my government argues that secret court rulings, which the world is not permitted to see, somehow legitimize an illegal affair....I

believe in the principle declared at Nuremberg in 1945: Individuals have international duties which transcend the national obligations of obedience. Therefore individual citizens have the duty to violate domestic laws to prevent crimes against peace and humanity from occurring."

Snowden said that the system for reporting problems does not work. "You have to report wrongdoing to those most responsible for it." He pointed out the lack of whistleblower protection for government contractors, the use of the 1917 Espionage Act to prosecute leakers, and his belief that had he used internal mechanisms to 'sound the alarm', his revelations "would have been buried forever." That sounds about right to us.

What is his future?

Simply put, it is bleak. He lives in a secret location in Russia, where Putin is no doubt happy to have him be a continuing irritant to the United States. Russia was certainly not on Snowden's list of places to land, but he had little choice once his passport was revoked while in the Moscow airport. His temporary asylum can be renewed annually and probably will be.

Was is worth it? Would he do it again? And what are law firms to make of his revelations?

Clearly, he believes it was worth it. He has made a difference insofar as there is intense scrutiny by many, including law firms, of potential "watchers" foreign and domestic. And we think a man who keeps a copy of the Constitution on his desk to refute superiors – yes, we think he'd do again – in a heartbeat.

As for lawyers, there are high level talks going on at many major law firms and a lot of chatter on the wire about the need to keep sensitive data out of e-mail, telephone conversations and video conferencing systems. Perhaps lawyers will actually use encryption to protect their client's confidential data and communications instead of constantly complaining that it is too difficult.

We think there is a strong likelihood that distrust of state-sponsored surveillance will have us harking back to the old days of face-to-face communication in places unlikely to have camera or audio surveillance. Graffiti on in a rest room stall at a

McDonald's resonated with author Nelson: It said simply "Orwell was Right." And so he was.

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