PROACTIVE BUSINESS STRATEGIES IN THE WAKE OF MASS SURVEILLANCE UNDER THE FEDERAL INTELLIGENCE SURVEILLANCE ACT

Carol M. Bast*

I. INTRODUCTION

He leaves his cellphone and laptop at home and instead brings "loaner" devices, which he erases before he leaves the United States and wipes clean the minute he returns. In China, he disables Bluetooth and Wi-Fi, never lets his phone out of his sight and, in meetings, not only turns off his phone but also removes the battery, for fear his microphone could be turned on remotely. He connects to the Internet only through an encrypted, password-protected channel, and copies and pastes his password from a USB thumb drive. He never types in a password directly, because, he said, "the Chinese are very good at installing key-logging software on your laptop."[1]

One might be surprised to learn that the above actions were not those of an undercover agent in a suspense thriller movie, but those of a knowledgeable business person traveling internationally, especially to Russia or China.[2] For example, the

[*] Associate Professor of Legal Studies, Department of Legal Studies, University of Central Florida, Orlando, Florida 32816.

[1] Nicole Perlroth, *Traveling Light in a Time of Digital Thievery*, N.Y. TIMES, Feb. 10, 2012, *available at* http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?_r=1. Instead of being the actions of someone in a futuristic spy movie, these are the measures taken by Kenneth G. Lieberthal of the Brookings Institute, a China experts who advises those on business trips. *Id.*

[2] The 2013 Verizon report was able to correlate approximately three quarters of the security breaches with the forty countries in which the breaches originated and found "that motive correlates very highly with country of origin." VERIZON, 2013 DATA BREACH INVESTIGATIONS REPORT 21 (2013), *available at* http://www.verizonenterprise.com/DBIR/2013/. Although the motive of seventy-five percent of the security breaches was financial gain, the motive of a sizable nineteen percent of the perpetrators were state-affiliated actors, presumably with espionage in mind. *Id.* at 5, 6. The report defined "espionage" as "state-sponsored or affiliated actors seeking classified information, trade secrets, and intellectual property in order to gain national, strategic, or competitive advantage. The only exception is when it is used for internal actors, where it refers to industrial espionage perpetrated by the employees of the victim." *Id.* at 11 n.9. "The majority of financially motivated incidents involved actors in either the U.S. or Eastern European countries (e.g., Romania, Bulgaria, and the Russian Federation). 96% of espionage cases were attributed to threat actors in China and the remaining 4% were unknown." *Id.* at 21.

Chairman of the United States House of Representatives House Intelligence Committee described himself as "electronically naked" while making such trips.[3] Presumably, the fear of many in business when traveling internationally is that they will be targeted for theft of trade secrets or financial gain.

Prior to 2013, a business might have been more concerned by privacy threats originating from the international arena, as alluded to above, than domestic privacy threats. However, that changed early in the summer of 2013. The summer and fall of 2013 presented a series of revelations concerning National Security Agency (NSA) mass surveillance[4] and NSA access to user data under the Foreign Intelligence Surveillance Act (FISA).[5] Through news reports, the public learned that the NSA was gathering telephone metadata, was accessing Internet traffic, was monitoring some communication within three hops of a terrorist target, and was accessing some mainstream software through backdoors into the programs.[6]

One of the consequences of these revelations was a shift in the public's attitude toward and knowledge of the extent of NSA activities; the public began to realize that, with NSA's tempting capability, the NSA might use technology for purposes other than gathering foreign intelligence.[7] For example, a Pew survey conducted in

[3] Perlroth, *supra* note 1. One might think of protecting sensitive data by encryption but both China and Russia outlaw encrypted data unless allowed by the government. *Id. Also see Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence*, 112th Cong. (2012)(statement of James R. Clapper, Director of National Intelligence), *available at* http://www.intelligence.senate.gov/120131/clapper.pdf.

[4] *See* James Bamford, *They Know Much More Than You Think*, N.Y. REV. BOOKS (Aug. 15, 2013), http://www.nybooks.com/articles/archives/2013/aug/15/nsa-they-know-much-more-you-think/?pagination=false; Ewen Macaskill & Gabriel Dance, *NSA Files: Decoded; What the revelations mean for you*, GUARDIAN, Nov. 1, 2013, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

[5] 50 U.S.C.A. §§ 1801 – 1885c (West, Westlaw through P.L. 113-174).

[6] *See* Macaskill & Dance, *supra* note 4. The NSA exploitation of software vulnerabilities is one example of the government's conflict between preventing cyberattacks and gathering intelligence information. An ACLU technologist commented, "If cybersecurity is, in fact, a big threat, then our government should be doing everything in its power to make sure that systems are as safe and secure as possible against all adversaries." Tom Gjelton, *Technology Outpacing Policymakers, Needs Of NSA* (NPR radio broadcast Nov. 19, 2013) *available at* http://www.npr.org/blogs/alltechconsidered/2013/11/19/246049281/technology-outpacing-policymakers-needs-of-nsa. The technologist added, "But what we've learned is that the NSA is willing to weaken the security of systems and software used by U.S. companies because it gives them an edge in surveillance." *Id.*

[7] NSA technology capability allows NSA employees to conduct unauthorized surveillance for reasons other than gathering foreign intelligence. For example, a letter from the NSA Inspector General to United States Senator Chuck Grassley detailed twelve incidents investigated by the Inspector General's office in which NSA employees abused NSA

mid-July 2013 showed that seventy percent thought that the NSA was not limiting its collection to terrorism investigation and fifty-six percent thought that the judiciary oversight was insufficient in curtailing NSA collection of telephone and Internet data. [8] The same Pew survey showed that, for the first time since the question was asked in 2004, more respondents were concerned that the government War on Terror had restricted civil liberties (47%) than those who were concerned that the government stance on terrorism had not gone far enough in protecting the country from terrorism threat (35%).[9]

Another consequence was a renewed interest in safeguarding privacy, with this interest coming both from the consumer and the business holding consumer data. An online Washington Post survey showed that, "In an atmosphere of increased concern about surveillance, users have adopted privacy-enhancing technologies, ditched services they deemed to have inadequate privacy protections, and even cut back on using the Internet for sensitive communications altogether."[10] Consumer trust is a

surveillance tools for personal reasons, such as to monitor the communication of a person with whom the NSA employee was having a relationship. Paul Lewis, *NSA employee spied on nine women without detection, internal file shows*, GUARDIAN, Sept. 27, 2013, *available at* http://www.theguardian.com/world/2013/sep/27/nsa-employee-spied-detection-internal-memo. As these twelve instances were only ones investigated and substantiated by the Inspector General's office, one might wonder how many other unauthorized surveillance incidents occurred but were undetected.

[8] PEW RESEARCH CENTER, FEW SEE ADEQUATE LIMITS ON NSA SURVEILLANCE PROGRAM; BUT MORE APPROVE THAN DISAPPROVE 1 (2013), *available at* http://www.people-press.org/files/legacy-pdf/7-26-2013%20NSA%20release.pdf. Of those who believed that the government was collecting data for purposes other than its anti-terrorism effort, the reasons for collection ranged from spying or being nosy (19%), gathering evidence on crimes other than terrorism (16%), monitoring (14%), collecting evidence for political purposes (13%), collecting information for whatever the government wants (10%), selling collected information (2%), enforcing taxes (1%), and targeting interest and religious groups (1%). *Id.* at 4.

[9] *Id.* at 2. A former NSA general counsel commented:

> The technology is moving very fast. . . . Legislation moves very slowly. Policy moves pretty slowly. The people who write policy don't always understand technology, and the people who write legislation almost never understand technology. And so in an era when the technology is moving quickly, it's really hard for the policy to keep up with it.

Gjelton, *supra* note 6.

[10] Timothy B. Lee, *Here's how people are changing their Internet habits to avoid NSA snooping*, WASH. POST, Nov. 7, 2013, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/07/heres-how-people-are-changing-their-internet-habits-to-avoid-nsa-snooping/. Responses indicated that users started to avoid cloud services, changed to independent search engines from main-stream ones, installed privacy enhancing software to protect their computers, and used a tool to block cookies. *Id.*

vital, but fragile, asset that the business must safeguard; in 2013, perhaps more than ever previously, consumers began to wonder how well their personal information was being protected by the businesses in which the consumers had entrusted their personal information.

Although the Snowden disclosures brought privacy concerns into the news on an almost daily basis in the latter half of 2013, prior to 2013 certain business leaders had anticipated the privacy challenges that a transition to digital worldwide communication might present and had taken certain measures to plan for the eventuality of an unauthorized breach into a company's proprietary and otherwise sensitive information. Lessons can be learned from the Snowden disclosures, with a business increasingly taking proactive steps to protect the privacy of business property, employees, and clients. These measures, more fully described below, include using the services of a privacy professional, either within the business or as a consultant, developing a privacy policy, implementing an information technology crisis management plan, and taking other proactive steps to protect business information.

II. Data Breaches

A starting point is to learn about the types of data breaches that are reported to have taken place. A 2013 report on data breaches divides breaches into "targeted," where an identified business is studied to identify technology weaknesses, and "opportunistic," where a technology weakness is exploited, with only one quarter targeted and three quarters of the breaches opportunistic.[11] "[S]ome organizations will be a target *regardless* of what they do, but most become a target *because* of what they do (or don't do)."[12] A variety of actions contributed to the data breaches, with several actions contributing to many data breaches.[13] Malware was a factor in forty percent of the breaches,[14] hacking in fifty-two percent,[15] social engineering in twenty-nine percent,[16] misuse in thirteen percent,[17] physical threats in thirty-five

[11] Verizon, *supra* note 2, at 48. These percentages varied little between large and small businesses, with 73% opportunistic breaches for large businesses and 74% for small businesses and 27% targeted breaches for large businesses and 26% for small businesses. *Id.*

[12] *Id.*

[13] *Id.* at 26.

[14] *Id.* at 29. "Malware is any **mal**icious soft**ware**, script, or code added to an asset that alters its state or function without permission." *Id. Also see* Microsoft Corporation, Security Intelligence Report (2013), *available at* http://www.microsoft.com/security/sir/default.aspx.

[15] Verizon, *supra* note 2, at 34. "Hacking includes all attempts to intentionally access or harm information assets without (or in excess of) authorization by circumventing or thwarting logical security mechanisms." *Id.*

[16] *Id.* at 36. Social engineering includes phishing or other actions taking advantage of human nature. *Id.* Phishing involves sending an email in the hopes that the recipient will take the "bait" by clicking on an email hyperlink or providing personal or financial information. The

percent,[18] and error in two percent.[19]

Another important factor in data breaches is the difficulty the perpetrator encounters in the initial breach of a business and subsequent breaches. As far as the initial breach is concerned, seventy-eight percent are of low or very low difficulty and the balance are of moderate difficulty. In considering a subsequent breach, seventy-three percent are of low or very low difficulty, seven percent are of moderate difficulty, and twenty-one percent are of high difficulty.[20] In 2012, sixty-six percent of the breaches were discovered months or more after the breach initially occurred and seventy percent were discovered by those external to the businesses, including third parties, auditors, customers, and law enforcement personnel.[21]

Prior to the disclosures of the summer of 2013, some leading businesses had taken privacy protection seriously by adopting privacy policies, as implemented by chief privacy officers. The role of the chief privacy officer, sometimes known as a chief security officer, is discussed the following section. The author suggests that businesses professionalize their interaction with technology, either by following in the path of industry leaders and creating a separate internal department of the business entrusted with implementing a business privacy policy or by seeking the same expertise from a privacy consultant; in addition, the best privacy practices must

report provides the following information:

> Running a campaign with just three e-mails gives the attacker a better than 50% chance of getting at least one click. Run that campaign twice and that probability goes up to 80%, and sending 10 phishing e-mails approaches the point where most attackers would be able to slap a "guaranteed" sticker on getting a click. To add some urgency to this, about half of the clicks occur within 12 hours of the phishing e-mail being sent.

Id. at 38. The 2014 Verizon report compared the likelihood of an email recipient clicking on an attachment (8%) and clicking on a link contained in email text (18%). VERIZON, 2014 DATA BREACH INVESTIGATIONS REPORT 47 (2014), *available at* http://www.verizonenterprise.com/DBIR/2014/. *Also see* ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS REPORT 2ND QUARTER 2014 (2014), *available at* http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf.

[17] VERIZON, *supra* note 2, at 36. Misuse is "[w]hen privileged parties maliciously or inappropriately use organizational resources in ways they should not." *Id.*

[18] *Id.* at 40. "Physical threats encompass deliberate actions that involve proximity, possession, or force." *Id.*

[19] *Id.* at 41. "We record an error as a threat action only if it deviates from normal processes within an organization and directly causes or significantly contributes to the incident." *Id.*

[20] *Id.* at 49. The report contains the comment, "Would you fire a guided missile at an unlocked screen door?" *Id.*

[21] *Id.* at 52, 53, 54.

be tailored to the size and type of business, the technology used by the business, and the type of data sought to be protected against breach.

III. CHIEF PRIVACY OFFICER

For industry leaders, the interaction of business stakeholders among each other and with technology has "required the implementation of privacy practices that were dynamic and forward-looking" with those leaders taking "a harm-avoidance approach" in ensuring the continued trust of the customer.[22] For them, implementation of practices to safeguard privacy is increasingly woven into the business structure at its most core level. Thus, "privacy within the firm has moved out of the closet and become a strategic concern" of doing business.[23]

A recent survey of industry leaders showed that, in the past twenty years, the digital technology landscape has changed and so has the way in which leading businesses handle privacy, with perhaps no more significant change than the professionalization of the privacy officer and the addition of a Chief Privacy Officer as an officer near the top of the corporate ladder.[24] The role of the Chief Privacy Officer is "'to take a much more forward look' aimed at identifying 'solutions that we could think about to develop that are not even on perhaps the drawing board right now.'"[25]

The International Association of Privacy Professionals, whose predecessor organization was formed in 2000, has become central in its role of providing education, certification, and networking opportunities to its members.[26] In addition, organizations external to a business often perform privacy audits and oversee compliance with business privacy policies.[27] Privacy protection in this realm has the dual focus of safeguarding the trust of the business customer and preventing breaches of databases containing confidential information, both as business strategies.[28] "Privacy . . . has evolved over the last several years to be defined in large part by respect for what consumers expect regarding the treatment of their

[22] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 269 (2011). The survey highlighted "identifying consumer expectations as a touchstone for developing corporate privacy practices beyond strict regulatory compliance." *Id.* at 270.

[23] Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance, Chief Privacy Officers, and*
the Corporate Management of Information Privacy in the United States: An Initial Inquiry, 33 LAW & POLICY 477, 504 (2011).

[24] Bamberger & Mulligan, *supra* note 22, at 251, 252.

[25] Bamberger & Mulligan, *supra* note 23, at 490.

[26] *About the IAPP*, INT'L ASS'N PRIVACY PROF., https://www.privacyassociation.org/about_iapp (last visited Nov. 17, 2014).

[27] Bamberger & Mulligan, *supra* note 22, at 262-63.

[28] *Id.* at 252.

personal sphere."[29]

The Chief Privacy Officer has the risk management function of gauging and preventing privacy harms involving the business, which necessarily means that the officer must be attentive to forces external, as well as internal, to the business. "Faced with uncertainty as to external demands on the firm resulting from the interplay between norms, technical and business changes, and flexible regulatory authority, they spend up to half of their time interacting with external stakeholders including regulators, advocates, and professional peers."[30] Thus, the Chief Privacy Officer is instrumental in evaluating the environment external to the business and implementing privacy practices in the business. Part of the implementation is ensuring that employees are trained to identify and appropriately deal with privacy issues that may arise.

Along with the professionalization of the role of the corporate privacy officer and the integral role of technology, came the rising importance of privacy advocates and the discussion of business privacy concerns by the media. This recently-formed "privacy community" was active and "pressed privacy as an issue" way before the 2013 disclosures of mass government surveillance.[31] The amount the discussion of privacy issues appears in the financial news has a significant effect on the attention that the top corporate officers place on emphasizing privacy implementation within the business;[32] since June of 2013, implementing a privacy policy has certainly been on the radar if not in the cross hairs of corporate board room discussions.

The networking on privacy concerns, both among privacy professionals and among businesses, plays a vital role in a business dealing with protecting privacy in the face of rapidly emerging technology. Rather than being competitive in this venture, privacy officers "reported that helping competitors make better privacy decisions was in their interest."[33] One privacy officer explained that "[h]elping 'my competitor at XYZ Company do better,' one described, . . . is not 'about competitive advantage.' Rather, '[t]hat's about doing the right thing because if they screw up . . .

[29] *Id.* at 270.

[30] Bamberger & Mulligan, *supra* note 23, at 479.

[31] Bamberger & Mulligan, *supra* note 22, at 277.

[32] One survey respondent noted:

> right now, you see the P word all over the place. [I]t used to be like once a week I'd cut out an article and say, 'Look, they're talking about privacy in the paper on page twenty-two of the Wall Street Journal.' And now it's pretty much every day. So I think we've won the battle of actually being noticed.

Id.

[33] *Id.* at 278.

it screws up all of us.'"[34] The avenues of success in the digital environment are prevention, detection, and reporting of breaches.[35]

A regular schedule of formal networking between those responsible for information technology security and the various departments or divisions of a business is also recommended, perhaps on a monthly or quarterly basis. Among other topics, the networking provides an opportunity for review of the business' continuity and recovery plans. A security consultant commented, "Security is not a department. It's an architecture. . . . These links are part of your security program – an evolving part of your ability to respond. It's observe, orient, decide, act. It's a living thing."[36]

IV. Business Security Planning

Thus, perhaps the biggest pay-off for the typical business is to implement basic preventative measures on a consistent basis. Preventative measures include adopting a privacy policy and a crisis management plan.

One security professional commented, "Any data-centric approach must incorporate encryption, [cryptographic] key management, strong access controls, and file monitoring to protect data in physical data centers, virtual and public clouds, and provide the requisite level of security."[37] The professional continued, "Today, it is table stakes to 'firewall the data'. By implementing a layered approach that includes these critical elements, organizations can improve their security posture more effectively and efficiently than by focusing exclusively on traditional network-centric security methods."[38] The following paragraphs contain a cursory description of some basic preventative measures.

The business should have a comprehensive privacy policy that is reviewed and updated on a regular basis so as to cover changes in technology, changes in the business, and acquisition of new technology.[39] An inventory should be maintained

[34] *Id.*

[35] One report advocates "focus on better and faster detection through a blend of people, processes, and technology" coupled with a call to "[c]ollect, analyze and share incident data to create a rich data source that can drive security program effectiveness." VERIZON, *supra* note 2, at 7.

[36] Illeana Armstrong, *Preparing for the new norm: 2013 Guarding against a data breach survey*, SC MAG., Mar. 2013, *available at* http://www.scmagazine.com/preparing-for-the-new-norm-2013-guarding-against-a-data-breach-survey/article/280934/.

[37] *Id.*

[38] *Id.*

[39] A 2010 United States Supreme Court case highlights an employer's failure to update its policy concerning technology so as to cover after acquired equipment; an additional problem was that there was a conflict between the written policy and a statement made by a supervisor. City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2625 (2010). In *Quon*, the city had a 2000

of all the business's electronic devices and software used on the devices, with devices and software kept appropriately current. An inventory should be maintained of the business' proprietary and confidential information, with such information secured to appropriate location.

Cloud computing, storing business information off-site with a cloud provider may need to be re-evaluated in the wake of the Snowden disclosures. "It is important to reiterate that jurisdiction still matters. Where the infrastructure underpinning cloud computing (ie, data centres) is located, and the legal framework that cloud service providers are subject to, are key issues."[40] Many businesses are performing that re-evaluation and, as a result, some ten to twenty percent of customers outside of the United States may move their information away from United States cloud providers.[41] One alternative may be for a business to go back to storing its information on-site rather than trusting it to a cloud. A second alternative would be to move the most crucial and sensitive information to an on-site location but leave the balance on the cloud.

In addition to a privacy policy, a business should have an information technology crisis management plan, both to prevent a security breach and to deal with a security breach, should one occur. The IT crisis management plan may include the following elements:

1. **Damage Assessment-** How you intend to ascertain exactly what has happened.
2. **Public Relations-** How you intend to respond (since timeliness is critical).
3. **Need for Outside assistance-** Who is needed to assist you with this highly technical problem.
4. **Resources needed to cure** defects that allowed this breach to happen.
5. **How you intend to monitor** & prevent future reoccurrences.[42]

Computer Policy. Pagers, with text capability, were acquired in 2001. Although the SWAT team officers were verbally told in 2002 that the text messages were covered by the Computer Policy and the verbal statement was memorialized in writing, a subsequent statement by a department lieutenant conflicted with the written memo. *Id.* This inconsistency made it difficult to determine whether Quon had a reasonable expectation of privacy in his text messages. *Id.*

[40] Maija Palmer, *Cyber security: Privacy experts profit from Prism uproar*, FIN. TIMES, Oct. 15, 2013, http://www.ft.com/cms/s/0/742baacc-25f7-11e3-8ef6-00144feab7de.html#axzz2j8amaT9z.

[41] *Id.*

[42] Lawrence J. Trautman, Jason Triche & James C. Wetherbe, *Corporate Information Technology Governance Under Fire*, 8 J. STATEGIC & INT'L STUD. 105, 110 (2013).

A law firm's ability to attract new clients is increasingly dependent on the law firm having an IT crisis management plan in place and this may be happening in other businesses as well. A law firm Chief Information Officer stated, "We'll get requests about our response plan in the event of a cyber-breach. . . . So [now] we have a cyber-response plan." A wise practice to test the effectiveness of the IT crisis management plan might be to either hire an outside firm to stage a mock security breach or to have the business conduct a mock security breach as a training exercise.

V. EMPLOYEES

As the recent report on security breaches[43] shows, three quarters of security breaches are opportunistic and the factors leading to initial security breaches are of a very low or low difficulty in approximately three quarters of the incidents. In addition, although ninety-two percent of the confirmed security breaches were attributed to outsiders, sixty-nine percent of security incidents were attributable to insiders.[44] One law firm Chief Information Officer commented, "The biggest gap in security is people," and then added: "That's where you are vulnerable."[45] This means that a business should take care in hiring and training employees.

Employee hiring should include appropriate background investigation. Employees should be educated on the privacy policy and trained to implement security procedures. Although these must be tailored to the particular business, basic security procedures may include: limitation on printing sensitive information, limitation on access to business devices or sensitive information by others, use of appropriate passwords, treatment of emails, links in emails, and email attachments, limitation on access to Internet sites, limitation on downloading online software or information, limitation on storage of sensitive information on portable devices, and storage and treatment of devices and business proprietary and confidential information.

[43] VERIZON, *supra* note 2, at 48.

[44] *Id.* at 20.

[45] Alan Cohen, *2013 Am Law Tech Survey: Firms' Data Security Fears Rise*, AM. LAW., Nov. 1, 2013, http://www.americanlawyer.com/PubArticleTAL.jsp?id=1202473327555&kw=2013%20Am%20Law%20Tech%20Survey%3A%20Firms%27%20Data%20Security%20Fears%20Rise&et=editorial&bu=National%20Law%20Journal&cn=20131104&src=EMC-Email&pt=Daily%20Headlines&slreturn=20131004163134. Phishing attacks have evolved into "spear phishing," which targets a particular organization or individual. Senior management is not immune from phishing attacks and "whaling" is a term coined to identify these phishing attacks. *See* Eric Basu, *Spear Phishing 101 - Who Is Sending You Those Scam Emails And Why?*, FORBES, Nov. 7, 2013, *available at* http://www.forbes.com/sites/ericbasu/2013/10/07/spear-phishing-101-who-is-sending-you-those-scam-emails-and-why/.

Physical access to business devices and sensitive information should be appropriately limited to certain individuals, at certain times, and at a certain frequency and the flow of data out of the network should be monitored to catch unusual occurrences. Limits on access should be reviewed and updated on a regular basis.

Perhaps the Snowden disclosures would not have happened without lapses in several of the measures recommended in the preceding paragraphs. It was reported that Snowden gained access to some of the documents in April of 2012 while working for Dell Inc. and gained access to additional material while working for Booz Allen Hamilton at the NSA facility in Hawaii beginning in late March or early April of 2013. Prior to Snowden's arrival in Hawaii, the federal government had begun to install software that could detect an unauthorized insider retrieving restricted information at various of its facilities. Because of the narrow bandwidth available at the NSA facility in Hawaii, the anti-leak software had not been installed at that facility.[46]

Information technology staff members, like Snowden, are tasked with making the technology system run smoothly and thus have "godlike access to systems they manage."[47] To accomplish this management mission, the system analyst must necessarily have some idea of the data flowing through the system; the system analyst may be a "super user" with "root access" to the technology system, allowing access to sensitive data without the high level clearance required if the system analyst was an intelligence agent.[48] For example, information on Bullrun, the NSA decryption program, was kept to the NSA chest, with analysts told, "Do not ask about or speculate on sources or methods underpinning Bullrun."[49] Those with sufficient clearance to have some knowledge of Bullrun were cautioned: "There will be no 'need to know'."[50] Even though agencies were warned to be "selective in which contractors are given exposure to this information," Snowden did obtain

[46] Mark Hosenball & Warren Strobel, *Exclusive: NSA delayed anti-leak software at base where Snowden worked*, REUTERS, Oct. 18, 2013, http://www.reuters.com/article/2013/10/18/us-usa-security-snowden-software-idUSBRE99H10620131018.

[47] Christopher Drew & Somini Sengupta, *N.S.A. Leak Puts Focus on System Administrators*, N.Y. TIMES, June 23, 2013, http://www.nytimes.com/2013/06/24/technology/nsa-leak-puts-focus-on-system-administrators.html?_r=0.

[48] *Id.*

[49] James Ball, Julian Borger, & Glenn Greenwald, *Revealed: how US and UK spy agencies defeat internet privacy and security*, GUARDIAN, Sept. 5, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[50] *Id.*

information on the program.[51]

Thus, the system analyst holds a special, privileged position with respect to the technology system. "In the classified world, there is a sharp distinction between insiders and outsiders. If you've been cleared and especially if you've been polygraphed, you're an insider and you are presumed to be trustworthy."[52] A system analyst working outside the classified world still may be regarded similarly as one to be trusted. Unfortunately, a rogue insider might take advantage of this trust to the detriment of the employer. Snowden may have gained access to sensitive information by using this position of trust to access information he would not otherwise had access. Apparently, some twenty to twenty-five of Snowden's co-workers turned over their usernames and passwords under Snowden's ruse that he needed the usernames and passwords to perform his duties as a system analyst.[53]

Methods to curb abuse of the system analyst's access to core, sensitive information might include especially careful vetting of the background of those being hired, including a review of any online posting the applicant may have done, and additional checks on the system analyst's access to crucial information, such as a requirement that two system analysts, rather than a sole system analyst, be required to approve access to crucial information. With top secret information, observation of the information technology employee may continue while the employee is on the job so as to note any signs that the employee is less than loyal to the employer. It may also be wise for the employer to evaluate the system analyst's legal relationship to the employer. The employer may have less control over the activities of someone who, like Snowden, was an employee of the contractor rather than a direct employee.[54]

VI. PROACTIVE STEPS

One computer expert says that if an individual or a business becomes a NSA "high-value target," NSA can use its "huge capabilities" to conduct surveillance of your communication; "if it wants in to your computer, it's in."[55] However, just as it is expensive to implement an elaborate kill chain approach, described below, to preventing security breaches, it is expensive for NSA to implement surveillance

[51] *Id.*

[52] Mark Hosenball & Warren Strobel, *Snowden is said to have tricked NSA co-workers into giving him their passwords*, WASH. POST, Nov. 7, 2013, http://www.washingtonpost.com/world/national-security/exclusive-snowden-persuaded-other-nsa-workers-to-give-up-passwords--sources/2013/11/07/6bfa9a54-4828-11e3-bf0c-cebf37c6f484_story.html.

[53] *Id.*

[54] Drew & Sengupta, *supra* note 47.

[55] Bruce Schneier, *NSA surveillance: A guide to staying secure*, GUARDIAN, Sept. 6, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance.

technology, including decrypting encrypted communication. "The NSA has turned the fabric of the internet into a vast surveillance platform, but they are not magical. They're limited by the same economic realities as the rest of us, and our best defense is to make surveillance of us as expensive as possible."[56]

When interviewed, Snowden stated, "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."[57] An easier route to access a target's communication than decryption is for NSA to gain access through an unsecure endpoint, meaning the target's computer, software, or network.[58] In the same interview, Snowden stated, "Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it."[59] It then follows that the target's first line of defense against NSA access is for the target to secure its endpoint, and a second line of defense is for the target to encrypt its communication.

Obviously, it would be better to avoid becoming an NSA target in the first place by remaining below the NSA radar. One might make oneself anonymous online by using Tor[60] or something similar, encrypting data traveling online, encrypting sensitive data on a computer with an air gap from a network, and using both open-source software and public-domain encryption, each of which is less likely to have an NSA-friendly back door.[61] Another expert suggests encrypting emails, stored data, telephone conversations over the Internet, and online chat or instant messaging. In addition, use of a virtual private network can allow one to surf the Internet

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] Tor (originally "the Onion Router") allows one to anonymously navigate the Internet by routing communication randomly through servers located in various parts of the world. Timothy B. Lee, *Everything you need to know about the NSA and Tor in one FAQ*, WASH. POST, Oct. 4, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/. For a description of how Tor works, *see* Eric Geier, *How (and why) to set up a VPN today*, PC WORLD, Mar. 19, 2013, http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html.

[61] Bruce Schneier, *How to remain secure against NSA surveillance*, GUARDIAN, Sept. 5, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance. The choice of the encryption method used is crucial as indicated by the following comment of Ladar Levison. "Without Congressional action or a strong judicial precedent, . . . I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States." Nicole Perlroth, Jeff Larson, & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 5, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0.

anonymously and mask an IP address.[62]

The business network and business devices should be configured, perhaps with sensitive data in a segmented and well-protected area of the network, to prevent or limit privacy breaches and should be audited and updated on a regular basis.[63] Devices and information can be protected by passwords, firewalls, virtual private networks, encryption, and anti-malware software. Disposal of business devices and information should be accomplished by appropriate digital and physical shredding of data. A business would be wise to forestall a security breach being made through an "open door" in the business' network. This open door "may come in the form of insecure remote-access services that are public-internet-facing and are not locked down" and "may also be exposed through vulnerabilities in the company's software or through an inexcusably weak password for a system that has long been forgotten."[64]

A security professional may discuss with a business the danger of advanced persistent threats (APT) faced by a targeted business. APT are "highly targeted, long-term, international espionage and sabotage campaigns by covert state actors."[65] The typical stages of APT are incursion, discovery, capture, and exfiltration. During incursion, the perpetrator breaks into the business network, often by using a social engineering scheme. During the discovery phase, the perpetrator explores the business network to spot the existence of vulnerable information and to determine the optimum methods of attack. The capture phase, which involves capturing sensitive information, may proceed for some time undetected. During exfiltration, the captured information is transmitted out of the business so that it can be used by

[62] Jon Matonis, *5 Essential Privacy Tools For The Next Crypto War*, FORBES, July 19, 2012**,** http://www.forbes.com/sites/jonmatonis/2012/07/19/5-essential-privacy-tools-for-the-next-crypto-war/. Virtual private networks are sometimes used to link computers within a particular business; however, they can also be used to create a secure encrypted tunnel through the Internet. *See* Geier, *supra* note 60.

[63] For example, law firm Chief Information Officers expressed client concern with the law firm storing information on a cloud maintained by a company outside the law firm:

> The cloud isn't just magic and smoke; data is in a physical location, highly secured, with redundant backups. But law firms want to be able to say that the data a client entrusted to it is on their server, in their office—not on a server they can't even tell you where it is. They just can't get comfortable with that.

Cohen, *supra* note 45. An option might be a private cloud over which the business does maintain control.

[64] Trautman, Triche & Wetherbe, *supra* note 42, at 112.

[65] SYMANTEC CORP., ADVANCED PERSISTENT THREATS: A SYMANTEC PERSPECTIVE 1 (2011), *available at* http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf.

the perpetrator.[66]

A targeted business might implement a kill chain approach to security, especially a business wary of APT. To understand the basis behind this approach one might think of "a stereotypical burglary — the thief will perform reconnaissance on a building before trying to infiltrate it, and then go through several more steps before actually making off with the loot." The theory behind this approach, modeled on a military kill chain, is that an attack occurs in stages and the attack on the target can be thwarted at any one of the stages, although the object is to do so as early as possible so as to obviate increased time and costs necessary to repair any damage.[67] A business likely to confront a targeted security breach would be more likely to use this approach, rather than a business more prone to opportunistic attack, as the kill chain approach requires a significant investment in time and financial resources. "Using the Cyber Kill Chain to keep attackers from stealthily entering your network requires quite a bit of intelligence and visibility into what's happening in your network. You need to know when something is there that shouldn't be, so you can set the alarms to thwart the attack."[68]

VII. Lessons to Be Learned

> "[T]he mid-1990s [was] a transformative period for information and communication technology use and policy in the United States and globally. The birth of the Internet as a commercial medium and the need to respond to privacy challenges created by its global and data-driven nature altered the political discourse about privacy protection."[69]

The goal of high technology companies is to improve existing products and introduce new products to the public. As technology advances, so must a high tech company's measures to safeguard its customers' sensitive data against surveillance, whether it be from the NSA or others. With shifting sands underfoot, protection measures are a moving target and must ensure that links between networks are as well guarded as the networks. An example of this is the NSA collecting data from cables linking Google and Yahoo data centers. "Those data centers are kept highly

[66] *Id.* at 2-6.

[67] Lysa Myers, *The practicality of the Cyber Kill Chain approach to security*, CSO, Oct. 4, 2013, http://www.csoonline.com/article/740970/the-practicality-of-the-cyber-kill-chain-approach-to-security?page=1. The author comments, "If you don't stop the attack until it's already in your network, you'll have to fix those machines and do a whole lot of forensics work to find out what information they've made off with." *Id.*

[68] *Id.*

[69] Bamberger & Mulligan, *supra* note 22, at 251, 280.

secure using heat-sensitive cameras and biometric authentication, and companies believed the data flowing among centers was secure. [Google] began the process of encrypting this internal traffic before reports of N.S.A. spying leaked during the summer, and accelerated the effort since then."[70] Google's chief legal officer commented, "We have long been concerned about the possibility of this kind of snooping, which is why we have continued to extend encryption across more and more Google services and links."[71] The attorney was dismayed at the NSA access. "We are outraged at the lengths to which the government seems to have gone to intercept data from our private fiber networks, and it underscores the need for urgent reform."[72]

In the wake of the Snowden disclosures, some countries and regions have toyed with the idea of compartmentalizing digital communication by country or region, by setting up firewalls surrounding a certain geographical region, much as China has used its much-criticized "great firewall" to isolate its citizens' communications with the outside world.[73] For example, Brazil has plans to protect the privacy of its citizens by routing communication traffic locally and to set up a secure national email system.[74] This potential "Balkanization" of worldwide communication would allow a user to plan the route communication would take while being mindful of the geographical location of the route and the attendant legal environment along the route; however, the downside is that developing these mini-Internets may require a large infusion of capital to establish regional networks and data centers and the long-term effect may be to slow technological innovation and stifle worldwide communication.[75]

The idea of communicating through a network partitioned or even separate from the worldwide flow of communication on the Internet is not confined to certain countries or regions. Some, for example, have gone to setting up their own communication mesh networks that may be parallel to, but unconnected from, the Internet. A mesh network is made up of a number of wireless radio nodes, each programmed to work with the other nodes in the network.[76] This has been a solution in certain instances and in communities in which the telecommunications company

[70] Charlie Savage, Claire Cain Miller & Nicole Perlroth, *N.S.A. Said to Tap Google and Yahoo Abroad*, N.Y. TIMES, Oct. 30, 2013, http://www.nytimes.com/2013/10/31/technology/nsa-is-mining-google-and-yahoo-abroad.html?_r=0.

[71] *Id.*

[72] *Id.*

[73] Ian Brown, *Will NSA revelations lead to the Balkanisation of the internet?*, GUARDIAN, Nov. 1, 2013, http://www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet.

[74] *Id.*

[75] *Id.*

[76] *See* Dave Roos, *How Wireless Mesh Networks Work*, HOWSTUFFWORKS.COM, http://www.howstuffworks.com/how-wireless-mesh-networks-work.htm (last visited Nov. 19, 2014).

balked at extending service the "last mile" from the Internet backbone to isolated or low socio-economic communities, with some mesh networks growing to sizable proportions.[77] For example, the Athens Wireless Metropolitan Network serves more than 1,000 members and the Guifi Spanish network serves more than 21,000 members.[78]

In addition, an alternative mesh network might be used by a political dissident whose access to international communication is severely limited by a repressive regime or by those who wish to escape NSA surveillance. Commotion, "internet in a suitcase" software, was developed by New America Foundation's Open Technology Institute and allows the establishment of an encrypted, private mesh network.[79] A Commotion mesh network would remain secure as long as its encryption is secure or until it is connected to the Internet.

The proactive measures discussed in several sections above concentrate on establishing business practices that, if implemented on a consistent basis, should protect the business from most opportunistic breaches of low or very low difficulty. Another proactive measure not discussed above would be for the business to become politically active in pressing the business' representatives in Congress for legislation to curb NSA activities or to allow the Foreign Surveillance Court to have more oversight power over NSA activities. This political activism could range from writing letters to elected officials, to meeting with elected officials, to becoming active in a political action committee, to becoming a campaign contributor, to contributing to a campaign of an incumbent challenger.[80]

VIII. CONCLUSION

These days, even a seemingly low-level technology business would be hard pressed to conduct its business "off the grid," or, in other words, totally disconnected from technology and without any trace of a digital footprint. For most businesses, the contact with customers and suppliers and the flow of digital information among them is constant. Even before the Snowden disclosures of mass surveillance by the government, those on the cutting edge anticipated the necessity of action. For law firms, motivating factors include "tougher regulatory requirements, more security-conscious clients, and the more sophisticated techniques used by cyber-criminals,

[77] Clive Thompson, *How to Keep the NSA Out of Your Computer*, MOTHER JONES, Sept.-Oct., 2013, http://www.motherjones.com/politics/2013/08/mesh-internet-privacy-nsa-isp.

[78] *Id.*

[79] *Id.*

[80] *See* Heather Long, *Fed up with Congress over the NSA or shutdown? 5 tips to get your voice heard*, GUARDIAN, Oct. 27, 2013, http://www.theguardian.com/commentisfree/2013/oct/27/how-to-contact-congress-tips.

who are increasingly targeting law firms."[81]

In the interconnected world in which a business operates, the new norm is to be continually on guard against data breaches and take as many proactive measures as possible to safeguard business data and, thereby, preserve consumer trust. Failure to take such measures may create ripple effects felt outside the business. One security expert commented, "The economy is an interconnected web with many interdependencies."[82] The expert continued, "An attack on one or multiple pieces of that web can have widespread impact[s] on a country's welfare. Organizations that do not maintain diligence in this area make themselves the weakest link in the chain and put every other part of the web at risk."[83] Therefore, a wise move is for the business to seek guidance from a privacy professional whose task it is to keep informed about the latest developments in technology and for the business to implement effective methods of protecting the business against unwanted intrusion.

[81] Cohen, *supra* note 45.
[82] Armstrong, *supra* note 36.
[83] *Id.*