EDPACS
THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

2014 VOL. 50, NO. 1

PRIVACY AND SECURITY PART I: PRIVACY AND SECURITY IN THE CORPORATE WORLD

AL MARCELLA AND CAROL STUCKI

Abstract. This article is the first of three that will explore the issues of privacy versus security. This first article will cover the corporate side. The second in the series will explore personal privacy versus security, and the third installment will review the overlap from both sides corporate versus personal privacy: Who really owns your data?

Privacy . . . such a vexing concept.

Whose privacy? Yours? Theirs? Ours? Mine?

How one word, a concept, can create such anxiety, raise such emotion, cause so much tension, enrage so many people, is nothing if not astounding.

Living at the cusp of the 21st century in a fully wired world, truly one's privacy, the ability to be left alone and to move about without the fear or concern that one is being "observed," "tracked," "exposed," will be the stuff of lore, spoken about in revered tones by our ancestors, never again to be experienced by our children or our children's children.

We all exist as a mere set of data points, constructed wholly of unique (and sometimes not so unique) digital DNA. Harvesting, isolating, manipulating, and analyzing these digital DNA, our daily digital footprints of our lives, singularly or en mass, exposes each and every one of us to unwanted and unsolicited examination.

Examination for what cause, to serve what ends? This article series examines the impact and effects of a growing global demand for increased privacy, the influence of technology on the erosion of privacy, and a corporation's ability to remain competitive among the converging demands for security, privacy, and profits.

IN THIS ISSUE

- **Privacy and Security Part I: Privacy and Security in the Corporate World**
- **Vendor Risk Management Using COBIT 5**

Taylor & Francis
Taylor & Francis Group

This article is the first of three that will explore the issues of privacy versus security. This first article will cover the corporate side. The second in the series will explore personal privacy versus security, and the third installment will review the overlap from both sides corporate versus personal privacy: who really owns your data?

PRIVACY AND SECURITY?

Privacy is the "right to be let alone."
◆ *Samuel Warren and Louis Brandeis*

The erosion of privacy has profound implications both personally and professionally. Profound for the organizations we work with as well as the organization's customers and stakeholders. Privacy is both a constraint and an enabler. Privacy constrains how business is conducted and the way information is handled. On the other hand privacy enables information-rich business offerings and increases the value of data—personal and corporate.

Given the exponential growth in user dependency on technology, mobile technology in particular, individuals should expect to see continued aggressive and persistent attacks on their privacy. This includes personally identifiable information (PII) as well as attacks on the systems that store and process these data.

In the next five to ten years, corporations should be prepared for significant changes in technologies that will both greatly assist in the protection of data privacy and related PII. However, because there is opposition in all things, these new technologies will give criminals greater capabilities to launch attacks and acquire larger amounts of data through greatly refined and more targeted attacks.

These same technologies will provide data aggregators (i.e., data brokers) volumes more personal information with which to digitally mine and ultimately digitally profile individuals. At an estimated 7.153 billion living humans on Earthi we are rapidly headed to becoming 7.5 billion markets of one.

Private information, PII in particular, will continue its movement to becoming a commodity with a recognized economic value. The associative incentive thus increases for unauthorized third-parties to attempt to liberate data owners of their data. Is your company taking proactive steps to protect company data? Your customer data? Your employee data?

Our global society is becoming increasingly connected via existing and emerging technologies in ways that did not even exist two

years ago. Those connections are not as well controlled or secure as consumers might want to believe. Individual privacy data will become more accessible to all sorts of people (e.g., criminals), companies (e.g., Google), and governments (e.g., yes, ours and everyone else's).

Given the insatiable demand for newer and faster technologies and the ability to access data from virtually any spot on the planet, consumers in general continue to be: (a) increasingly blasé of the advances in technologies that will allow both authorized and unauthorized individuals to pry into their private life, accepting this as another cost of doing business in the 21st century; (b) less and less protective of their privacy and PII, if it means giving up elements, if not the entirety of their PII in order to obtain a free vendor discount coupon; (c) the primary point of targeted attacks, due to the fact that most individuals do not employ a defense in depth strategy strong enough to protect their most sensitive, private data.

"We have a saying in this business: Privacy and security are a zero-sum game."
◆ *Ed Giorgio*

These same individuals who are blasé about privacy protection may be working for your company and placing your organization at risk. The risk of data and privacy issues include: financial loss, legislative penalties, and a loss of costumer confidence.

Furthermore, the movement of data of all types, away from the direct control of the data owner into the hands of external third-party service providers creates new threats and exposures to the safeguarding of both personal privacy and PII. Hardening defenses may require unpopular decisions, financial expenditures, proactive revision of existing policies and procedures, and modifying the way in which one conducts daily activities, both professionally and personally. Most people, however, do not embrace change well.

In the IT audit and security field, there is the conflict that arises when attempting to find the proper balance between security, control, and privacy.

PRIVACY OR SECURITY—WHAT'S AT RISK?

What's at risk would depend on two things: (1) What data the company collects internally on its employees, partners, suppliers, contractors, and so on, and (2) What type of data the company collects about its customers. These are two different objectives for collection and security. Many purposes, exploding into infinity, for the use of this data can be derived. Along with the issues of collecting the data the company wants to first ensure it is accurate and useful. However, often overlooked is the protection of this data.

Depending on the type of data the ramifications of that data being accessed by unauthorized means or corrupted can have different consequences. For example, healthcare or financial data are highly regulated and breaches of security come with some severe penalties, not to mention reputational impact on the business. On the other hand, exposing consumer shopping habits may not have the same consequences.

So, let us first explore the internal company practices that may expose risk to the corporation. These exposures include employee use of company e-mail, Internet, and phones for personal use; practices of sharing data between business partners; internal

access to customer data; and practices in providing data to external sources.

Employees are the weakest link in security after all most are naïve to the ramifications of a few seemingly harmless interactions with data. Use of e-mail, even for company purposes, can lead to breaches of security. How? Joe e-mailed a copy of a customer list to his co-worker Jim. Jim's company phone, which he uses to access his company e-mail, is lost. The finder of the phone could access that e-mail with the customer data, especially if there is no password protection on the phone, e-mail account, or even on the file containing the customer data. These are simple points of access that could be easily prevented if employees practiced good security habits. Security habits that can be enforced by company polices and procedures, not to mention actual applications that reside on e-mail and phones to protect the loss of data by encrypting data and remote wiping of the device in the event it is lost or stolen.

There are numerous other security and privacy issues that can arise from employees abusing company e-mail, Internet, and phone use. Human Resources and IT Security should have policies and procedures for protecting company information not to mention employee information. How many company phones contain employee personal data? If there is no policy or practice to inform the employee the company phone is only for company use that employee could sue the company if his/her data is breached on that company phone, even if the phone is not lost but breached.

Other private data that the company keeps on its employees that needs to be secured includes employee benefits—especially healthcare and insurance information, financial information (most companies obtain a credit report on employees during the hiring process), performance evaluation information, and government identification information such as social security numbers.

Private data for business partners, suppliers, and contractors could include but is not limited to: credit or financial information, payment/banking information (bank account numbers and routing information), their list of customers, tax identification numbers, contracts, invoices with discount information, warranty agreements, and other competitive information.

What type of data being collected, available for assessment, and retained by the company depends mostly on the type of business. There are known strict regulations over healthcare information under the Health Insurance Portability and Accountability Act (HIPAA).

Likewise, there are regulations over privacy and security of financial information; the Gramm-Leach-Bliley Act is one of the most prevalent. Both of these acts require organizations to secure private data and will assess penalties for breaches. In addition to healthcare providers, insurance companies, and financial institutions there are many businesses that are impacted by some portion of these regulations.

The increasing expansion of global, Internet connected, mobile business, will require organizations to be cognizant of a multitude of international laws increasingly aimed at the protection of citizens' personal privacy, when entering new markets and releasing upgraded products and services (see Table 1).

Table 1 ***International Privacy Laws****

- **Argentina:** Personal Data Protection Act of 2000 (aka Habeas Data)
- **Austria:** Data Protection Act 2000, Austrian Federal Law Gazette part I No. 165/1999
- **Australia:** Privacy Act of 1988
- **Belgium:** Belgium Data Protection Law and Belgian Data Privacy Commission Privacy Blog
- **Brazil:** Privacy currently governed by Article 5 of the 1988 Constitution.
- **Bulgaria:** The Bulgarian Personal Data Protection Act, was adopted on December 21, 2001 and entered into force on January 1, 2002. More information at the Bugarian Data Protection Authority
- **Canada:** The Privacy Act - July 1983 Personal Information Protection and Electronic Data Act (PIPEDA) of 2000 (Bill C-6)
- **Chile:** Act on the Protection of Personal Data, August 1998
- **Colombia:** Two laws affecting data privacy - Law 1266 of 2008: (in Spanish) and Law 1273 of 2009 (in Spanish) Also, the constitution provides any person the right to update their personal information
- **Czech Republic:** Act on Protection of Personal Data (April 2000) No. 101
- **Denmark:** Act on Processing of Personal Data, Act No. 429, May 2000.
- **Estonia:** Personal Data Protection Act of 2003. June 1996, Consolidated July 2002.
- **European Union:** European Union Data Protection Directive of 1998
- EU Internet Privacy Law of 2002 (DIRECTIVE 2002/58/EC)With a discussion here.
- **Finland:** Act on the Amendment of the Personal Data Act (986) 2000.
- **France:** Data Protection Act of 1978 (revised in 2004)
- **Germany:** Federal Data Protection Act of 2001
- **Greece:** Law No.2472 on the Protection of Individuals with Regard to the Processing of Personal Data, April 1997.
- **Guernsey:** Data Protection (Bailiwick of Guernsey) Law of 2001
- **Hong Kong:** Personal Data Ordinance (The "Ordinance")
- **Hungary:** Act LXIII of 1992 on the Protection of Personal Data and the Publicity of Data of Public Interests (excerpts in English).
- **Iceland:** Act of Protection of Individual; Processing Personal Data (Jan 2000)
- **Ireland:** Data Protection (Amendment) Act, Number 6 of 2003
- **India:** Information Technology Act of 2000
- **Italy:** Data Protection Code of 2003 **Italy:** Processing of Personal Data Act, January 1997
- **Japan:** Personal Information Protection Law (Act) (Official English Translation) Law Summary from Jonesday Publishing
- **Japan:** Law for the Protection of Computer Processed Data Held by Administrative Organs, December 1988.
- **Korea:** Act on Personal Information Protection of Public Agencies Act on Information and Communication Network Usage
- **Latvia:** Personal Data Protection Law, March 23, 2000.
- **Lithuania:** Law on Legal Protection of Personal Data (June 1996)
- **Luxembourg:** Law of 2 August 2002 on the Protection of Persons with Regard to the Processing of Personal Data.
- **Malaysia:** Common Law principle of confidentiality Personal data Protection Bill (Not finalized) Banking and Financial Institutions Act of 1989 privacy provisions.
- **Malta:** Data Protection Act (Act XXVI of 2001), Amended March 22, 2002, November 15, 2002 and July 15, 2003
- **Mexico:** Federal Law for the Protection of Personal Data Possessed by Private Persons (Spanish) - The regulations deal with data subjects' rights, security and breach notification provisions, cloud computing, consent and notice requirements, and data transfers. Good summary of the law in English at the IT Law Group
- **Morocco:** Data Protection Act
- **Netherlands:** Dutch Personal Data Protection Act 2000 as amended by Acts dated 5 April 2001, Bulletin of Acts, Orders and Decrees 180, 6 December 2001
- **New Zealand:** Privacy Act, May 1993; Privacy Amendment Act, 1993; Privacy Amendment Act, 1994
- **Norway:** Personal Data Act (April 2000) - Act of 14 April 2000 No. 31 Relating to the Processing of Personal Data (Personal Data Act)
- **Philippines:** DATA PRIVACY ACT OF 2011 There is also a recognized right of privacy in civil law and a model data protection code.
- **Romania:** Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data
- **Poland:** Act of the Protection of Personal Data (August 1997)
- **Portugal:** Act on the Protection of Personal Data (Law 67/98 of 26 October)
- **Singapore:** The E-commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce. Other related Singapore Laws and E-commerce Laws.
- **Slovak Republic:** Act No. 428 of 3 July 2002 on Personal Data Protection.

Table 1 ***(Continued)***

- **Slovenia:** Personal Data Protection Act, RS No. 55/99.
- **South Africa:** Electronic Communications and Transactions Act, 2002
- **South Korea:** The Act on Promotion of Information and Communications Network Utilization and Data Protection of 2000
- **Spain:** ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data
- **Switzerland:** The Federal Law on Data Protection of 1992
- **Sweden:** Personal Data Protection Act (1998:204), October 24, 1998
- **Taiwan:** Computer Processed Personal data Protection Law- applies only to public institutions. (English Translation)
- **Thailand:** Official Information Act, B.E. 2540 (1997) for state agencies. (Personal data Protection bill under consideration)
- **United Kingdom:** UK Data Protection Act 1998 Privacy and Electronic Communications (EC Directive) Regulations 2003 official text, and a consumer oriented site at the Information Commissioner's Office.
- **Vietnam:** The Law on Electronic Transactions 2008

*"International Privacy Laws," Information Shield, 3503 Winter Crest Ct., Sugar Land, TX 77479, +1 888.641.0500, www.informationshield.com/intprivacylaws.html, retrieved April 2014, used with permission.

PRIVACY: ACCOUNTABILITY IN THE WORKPLACE

An individual's personal information is used by organizations for various business activities like market research, customer ratings, rights management, direct marketing, and data trading. It may also be of interest for the individual's community, friends, family, and professional network.

Personal information could also be collected and used by domestic and foreign governments, competitors, disgruntled employees, hackers, cyber-terrorists, saboteurs, identity thieves, and the like. Therefore, threats to data require organizations to protect personal information adequately, avoiding adverse consequences and litigation.

How effectively does your organization protect personal, private information? The private information of its clients, customers? Your private information held in the HR/Employee Services department? Exchanged with third-party contractors (e.g., payroll, medical)?

When was the last time a comprehensive privacy audit was undertaken in your organization?

Is your organization asking these top privacy control questions?

1. What privacy laws and regulations impact the organization?
2. What type of personal information does the organization collect?
3. Does the organization have privacy policies and procedures with respect to collection, use, retention, destruction, and disclosure of personal information?
4. Does the organization have responsibility and accountability assigned for managing a privacy program?
5. Does the organization know where all personal information is stored?
6. How is personal information protected?
7. Is any personal information collected by the organization disclosed to third parties?

8. Are employees properly trained in handling privacy issues and concerns?
9. Does the organization have adequate resources to develop, implement, and maintain an effective privacy program?
10. Does the organization complete a periodic assessment to ensure that privacy policies and procedures are being followed?ii

Adding a bonus question number 11 to this list: Enterprise-wide, what can your organization do to shorten its data retention cycle, thereby reducing the potential risk associated with these data?

Failure to properly address the protection of personal information presents a number of risks to the organization, including:

"You have zero privacy anyway. Get over it."
◆ *Scott McNealy*

- Possible damage to the organization's public image and branding
- Potential financial or investor losses
- Legal liability or industry or regulatory sanctions
- Charges of deceptive practices
- Customer, citizen, or employee distrust
- Loss of customers or revenues
- Damaged business relationships.iii

To avoid those consequences, any corporate entity that collects, uses, or transfers personal information must take steps to ensure it is complying with legal requirements for maintaining data privacy and— equally important—living up to the trust of its employees, customers, partners, and suppliers. A privacy audit provides a means of benchmarking corporate privacy practices against what the law requires and what industry best practices demand.iv

CONDUCTING A PRIVACY RISK/IMPACT ASSESSMENT REVIEW

Determining that your organization is in compliance with local, state, federal and international privacy legislation, reviewing privacy policies and procedures and substantiating this compliance, should be the main objective of an enterprise-wide privacy audit.

A good first step toward addressing privacy risks within an organization is through conducting a privacy risk/impact assessment (PIA). An excellent tool for this critical assessment process is the template jointly developed by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants (www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/item10752.aspx).

Learning about a weakness in your privacy program once a breach has occurred is too late (see Tables 2 and 3). The template mentioned above is an excellent starting point for a comprehensive internal privacy audit.

While a privacy impact assessment is a methodology for identifying risks to privacy posed by any new project, product, service, technology, system, program, policy, or other initiative and devising solutions to avoid or mitigate those risks, it also offers several important benefits to organizations, their employees, contractors,

Table 2 ***Top 20 Government-Imposed Data Privacy Fines Worldwide, 1999–2014****

Rank	Fined entity	Amount of fines and penalties	Year	Country	Privacy principles violated
1	Apple	$32.5M	2014	U.S.	Choice and Consent
2	Google	$22.5M	2012	U.S.	Collection
3	Google	$17M	2013	U.S.	Collection and Notice
4	ChoicePoint	$15M	2006	U.S.	Security
5	Hewlitt-Packard	$14,5M	2006	U.S.	Collection
6	LifeLock	$12M	2010	U.S.	Accuracy, Security
7	TJ Maxx	$9.8M	2009	U.S.	Security
8	Dish Network	$6M	2009	U.S.	Choice and Consent
9	DirecTV	$5.3M	2005	U.S.	Choice and Consent
10	HSBC	$5M	2009	UK	Security
11	US Bancorp	$5M	1999–2000	U.S.	Disclosure
12	Craftmatic	$4.3M	2007	U.S.	Choice and Consent
13	Cignet Health	$4.3M	2011	U.S.	Access
14	Barclays Bank	$3.8M	2013	U.S.	Use and Retention
15	Certegy Check Services	$3.5M	2013	U.S.	Accuracy
16	Playdom	$3M	2011	U.S.	Collection and Notice
17	The Broadcast Team	$2.8M	2007	U.S.	Collection
18	Equifax, TransUnion and Experian	$2.5M	2000	U.S.	Access
19	CVS Caremark	$2.3M	2009	U.S.	Security and Disposal
20	Norwich Union Life	$1.8M	2007	UK	Disclosure

*Cline, J. (February 17, 2014). "U.S. Takes the Gold in Doling Out Privacy Fines." *Computerworld*, www.computerworld.com/s/article/9246393/Jay_Cline_ U.S._takes_the_gold_in_doling_out_privacy_fines?taxonomyId=84&pageNumber=3 (retrieved April 2014), used with permission.

customers, citizens, and regulators. Among these benefits are the following:

- A PIA has often been described as an early warning system. It provides a way to detect potential privacy problems, take precautions, and build tailored safeguards before, not after, the organization makes heavy investments.
- Although a PIA should be more than simply a compliance check, it does nevertheless enable an organization to demonstrate its compliance with privacy legislation in the context of a subsequent complaint, privacy audit or compliance investigation.
- A PIA can help an organization to gain the public's trust and confidence that privacy has been built into the design of a project, technology, or service.
- An organization that undertakes a PIA demonstrates to its employees and contractors that it takes privacy seriously and expects them to do so too.
- A proper PIA also demonstrates to an organization's customers and/or citizens that it respects their privacy and is responsive to their concerns.v

Table 3 ***Top 10 Data-Privacy Lawsuit Settlements Worldwide, 1999–2014****

Rank	Entity Sued	Year	Amount of Award	Jurisdiction	Privacy Principles Violated
1	LensCrafters	2008	$20M	U.S. (California)	Disclosure
2	Facebook	2013	$20M	U.S. (California)	Choice and Consent
3	Facebook	2013	$9.5M	U.S. (California)	Collection, Disclosure
4	Netflix	2010	$9M	U.S. (California)	Retention
5	AOL	2013	$6M	U.S. (Virginia)	Disclosure
6	Time Warner	2009	$6M	U.S. (New York)	Choice and Consent
7	NebuAd	2011	$2.4M	U.S. (federal court)	Collection and Notice
8	TD Ameritrade	2009	$1.9M	U.S. (California)	Security
9	Minneapolis City Council, City of St. Paul, and other city governments	2012	$1.06M	U.S. (Minnesota)	Collection
10	Louis Vuitton	2013	$1M	U.S. (California)	Collection

*Cline, J. (February 17, 2014). "U.S. Takes the Gold in Doling Out Privacy Fines." *Computerworld*, www.computerworld.com/s/article/9246393/Jay_Cline_U.S._takes_the_gold_in_doling_out_privacy_fines?taxonomyId=84&pageNumber=3 (retrieved April 2014), used with permission.

"The American people must be willing to give up a degree of personal privacy in exchange for safety and security."
◆ *Louis Freeh*

"Doveryai, no proveryai"
◆ *Russian proverb "trust but verify"*

When was the last time your organization preformed an enterprise-wide privacy impact assessment? An internal privacy audit? Maybe it's time!

CONCLUSION

In the long run, the best approach to mitigating the loss of privacy is through ongoing, proactive training and vigilance.

Maintaining an ongoing awareness of current and emerging technologies and exploits designed to relieve your company of private, confidential data is the best approach for protection. Evaluate technology, assess exposures to private information, and implement those technologies (think mobile apps) that you have vetted and trust. Routinely perform enterprise privacy audits and respond immediately to identify exposures, weaknesses, and gaps.

Conduct continual training and have ongoing discussions with employees on the dangers and risks of disclosing not only PII but any personal, private information. Emphasize to always first verify and validate the authentication of an individual requesting any private information and then, the specific need and authorization for the collection of any proprietary data, prior to releasing these data.

Although this may be a logical analysis, it still begs the question . . . given the ever increasing and evolving sophistication of technology and the integration of these technologies into our daily, personal lives, exactly how comfortable are you with the erosion of your privacy as payment for your security?

To put it in a different light, how could that private information be used against your company? Is it worth the risk or price of your

company reputation or your job? Is the company putting your personal information at risk?

The latter question is explored in the second installment of this three part series on privacy and security.

Notes

i. World Population Clock as of March 17, 2014 at 10:06 CDT, www.census.gov/popclock (retrieved March 2014).
ii. Hahn, U., Askelson, K., & Stiles, R. (June 2006). "Global Technology Audit Guide 5: Managing and Auditing Privacy Risks," The Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, Florida 32701, www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/DownloadableDocuments/GTAG5PrivacyRisks.pdf (retrieved February 2014).
iii. Ibid.
iv. Whitener, M. (July 2012). "Conducting a Privacy Audit," *The Corporate Counselor*, *27*(3), 1.
v. Wright, D., Wadhwa, K., De Hert, P. and Kloza, D. (September 21, 2011). "A Privacy Impact Assessment Framework for Data Protection and Privacy Rights." Prepared for the European Commission Directorate General Justice, JLS/2009–2010/DAP/AG, www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf (retrieved February 2014).

Albert J. Marcella Jr., Ph.D., CISA, CISM, is president of Business Automation Consultants, LLC. Dr. Marcella, is an internationally recognized public speaker, researcher, and workshop and seminar leader with over 35 years of experience in IT audit, security, and assessing internal controls. Dr. Marcella, has authored numerous articles and 29 books on various IT, audit, and security related subjects.

Carol Stucki, CISA, PMP, is a Project Manager with over 25 years of experience in operational and IT roles including providing internal systems consulting, portfolio management, and auditing services for companies both in the Unites States and abroad. Carol has worked for GTE (now Verizon), Arthur Andersen, Perot Systems, Los Alamos National Labs on DOE, DOD, HSD contracts, Church of Jesus Christ of Latter-day Saints, Capgemini, and HealthNow.

EDPACS
THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

2014 VOL. 50, NO. 2

PRIVACY AND SECURITY PART II: IT'S PERSONAL

AL MARCELLA AND CAROL STUCKI

Abstract. This article is the second in a series of three that explores the issues of privacy versus security. The first article, "Privacy and Security Part I: Privacy and Security in the Corporate World" covered the corporate side. This second in the series will explore personal privacy versus security, and the third installment will review the overlap from both sides corporate versus personal privacy: Who really owns your data?

PRIVACY AND SECURITY?

Our global society is becoming increasingly connected via existing and emerging technologies in ways that did not even exist two years ago. Those connections are not as well controlled or secured as consumers might want to believe. Individual personal information will become more accessible to all sorts of people (e.g., criminals), companies (e.g., Google), and governments (e.g., yes, ours and everyone else's).

Significant changes in technologies that will both greatly assist in the protection of individual privacy and related PII are sweeping into society today and will continue to increase over the next five years. However, because there is opposition in all things, these new technologies will give criminals greater capabilities to launch attacks and acquire larger amounts of data through greatly refined and more targeted attacks.

These same technologies will provide data aggregators (i.e., data brokers) volumes more personal information with which to digitally mine and ultimately digitally profile individuals. At an estimated 7.153 billion living humans on Earth[i] we are rapidly headed to becoming 7.5 billion markets of one.

Private information, PII in particular, will continue its movement to becoming a commodity with a recognized economic value. The associative incentive thus increases for unauthorized third-

IN THIS ISSUE

- **Privacy and Security Part II: It's Personal**
- **Are All of Your Customers Profitable and Valuable to You?**

Taylor & Francis
Taylor & Francis Group

parties to attempt to liberate data owners of their data. Are you taking proactive steps to protect your PII? Your privacy?

A key element of privacy is the ability of each individual to control his or her own information, identity, and property. Although society could not function if each person demanded complete personal privacy, we all want to feel we have control over the amount and type of personal information others know about us.

The quest for privacy must not come at the expense of what can be described as "the right to know." Businesses have a right to know what their employees are doing on the job, governments have the right to know that public assets are being used for their intended purposes, and marketers have the right to identify customers who may be interested in buying their products. The goal is not to isolate oneself from society in order to maintain complete personal privacy; it is to live within society while still maintaining control over who sees your personal information.

The movement of data of all types, away from the direct control of the data owner into the hands of external third-party service providers creates new threats and exposures to the safeguarding of both personal privacy and PII. Hardening defenses may require unpopular decisions, financial expenditures, proactive revision of existing policies and procedures and modifying the way in which one conducts daily activities, both professionally and personally.

"Once you've lost your privacy, you realize you've lost an extremely valuable thing."
◆ *Billy Graham*

"Personal data is the new oil of the Internet and the new currency of the digital world."
◆ *Meglena Kuneva*

"A man's house is his castle."
◆ *Sir Edward Coke*

A PERSON'S HOME IS THEIR CASTLE—REALLY?

Article 8 of the European Convention on Human Rights includes the right to privacy, stating in context that everyone has the right to respect for his private and family life, his home, and his correspondence.

This expectation is facing a serious threat in credibility and enforcement, as technology becomes more pervasive and pries ever increasingly into our most private places—our homes.

Given the recent uptick in the increased, individual awareness of exactly how much privacy we (at least we here in the good ol' US of A) do not have, any movement to further encroach on an individual citizen's privacy is bound to polarize a populous be it a neighborhood, city, state, or nation. The following example emphasizes this polarization.

This example is a recent debate among a neighborhood regarding a proposal to install surveillance cameras at strategic intersections throughout the neighborhood. It has been interesting reading the blog exchanges between pro- and anti-camera neighbors. Those opposing the installation of cameras speak to the extended invasion of personal privacy and "government" (read authority) intervention. On the opposite side of the street (sometimes literally) there are voices touting safer streets, less pass-through traffic, a positive discouragement to unwanted or illegal behavior, and an added sense of security. The debate continues with no formal decision yet being reached. A decision once made predictably will be acceptable to only half the community residents.

Further contemplation about the claim of a greater sense of security against the backdrop of further relinquishing one's personal privacy, one can wonder exactly how comfortable, secure, and confident are we regarding the level of privacy we have within our own homes?

As professionals working in the IT audit and security field, we are acutely aware of the conflict that arises when attempting to find the proper balance between security, control, and privacy.

No security device or system will deliver 100 percent security or control (at least not one with a human interface component) and similarly, no privacy policy is 100 percent private. The potential, however, with a security system is to create doubt, hesitation, and raise the question in the mind of a potential criminal as to the vulnerability of a single home or (with prominently displayed street cameras), potentially an entire neighborhood.

As one of the pro-camera supporters blogged: "Security cameras are one element in a larger pro-active strategy that provides a potential deterrent and contributes to improving, increasing and sustaining community-wide security programs."

Those who may question their community's commitment to security versus privacy might just want to take a stroll around their neighborhood and tally the number of homes that have security system "lawn signs" and vendor window stickers prominently displayed around their home.

What are these lawn signs and stickers communicating to the potential criminal, even if subliminally? "Is the home protected or not, am I willing to take the chance, the risk, or just move on to another home, another neighborhood?" "Do I want to take the risk that the sign may be just a ruse and the home is not protected, or just go find an easier target?" We value our security and publicly admit to this via the signage we display on our properties.

It is surprising to see the number of "security signs" that have popped up around neighborhoods; there has certainly been an increase over the years.

"The virtue of privacy is one that must be protected in matters that are intimate and within one's own family."
◆ *Tiger Woods*

PRIVACY OR SECURITY—WHAT'S AT RISK?

Just how much privacy are we willing to give up for the sake of acquiring that peace of mind, that sense of security? Are these neighbors really aware of just how much privacy they are giving up in their quest for personal security? It makes one wonder if

these neighbors ever questioned what privacy they were giving up by installing that in-home security surveillance system.

Privacy advocates may try to point out that there is a difference between a private home security system and public security cameras;and there is, in their objectives, placement, and usage. However, the same individuals may be very surprised to learn of the "personal" information available, tracked, and eventually retained by those in-home security surveillance systems and their third-party security providers.

A quick analysis of the type of information that may be gleaned from inside your secure, private residence via your home security system, brings to mind such information as:

1. Your daily living patterns, when you leave, when you come home, when you move between rooms (motion detectors track your room-by-room movement).
2. When you go to sleep at night, wake up in the morning (when you turn on and when you turn off the alarm system, by setting off individual room motion detectors and fluctuations in room temperatures as you settle in for a good nights' sleep).
3. Your late night raids on the refrigerator (again setting off various room motion detectors).
4. The temperature in your home (some security monitoring companies sell a wide variety of "environmental monitoring" add-on devices/options that among other features, can detect a drop in home temperature).
5. Your financial information (credit history, payment plans, current or outstanding balances, bank account number or credit card number for repayment options) and by default, your credit score, payment history, and other potentially "linked" financial information.
6. Emergency and non-emergency (secondary) contact numbers of friends or other family members.
7. Your access passcode (which in many cases is short, simple, and selected on the basis of its ease to remember and enter when the entry alarm sounds; probably a family member's birthdate or numeric keypad pattern; e.g., 1590, 1236).
8. Your pass phrase to validate a false alarm or forced entry. Which again may be something very familiar and potentially linked to a pass phrase you use daily, say at work to access your secure desktop files.
9. Types and possible number of pets you may have, due to the sensitivity and type of motion detection devices installed (or not installed), and their location (either by height or specific home "zones").
10. Secondary access codes for service personnel, additional family members, and so on.
11. If you have opted for the "camera package," still images and video captured via cameras installed around and throughout the house and stored on your provider's server. Pictures of you, your family, your guests.
12. In more sophisticated monitoring systems, which provide both audio along with video surveillance, in rooms where such

devices are installed, recorded conversations will be stored on the service provider's server.

If you have the "app" to check your security system remotely, more of your private information available would include:

13. Your mobile phone number.
14. Your Global Positioning System (GPS) location information. Includes where you have been.
15. Your call history log.
16. The amount of energy you are conserving (or wasting) via appliances that are turned on or off remotely or via the system's pre-programmed "options."
17. Potentially any other information currently being gleaned from your mobile device without your authorization or knowledge.

We have identified just a few data that are potentially being collected, monitored, and retained regarding your activities inside your private home.

Did you know that these type of data are being collected, available for assessment, retained by your home security service provider? Have you asked?

- What does your provider do with these data?
- How long are these data retained?
- How are these data secured?
- Who has access to these data outside of the provider's need-to-know employees?
- Could any of these data be shared or sold to third-party providers (e.g., pet service providers, boarding kennels, landscapers, and baby sitters, Heating, Ventilation, and Air Conditioning (HVAC) contractors [our monitoring of your furnace indicates that it is not functioning properly and should be serviced], your insurance company, etc.)?

"Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."
◆ *Louis D. Brandeis*

STIRRING UP A PRIVACY HORNET'S NEST

As increasing human desire, need, and drive for real-time, global, instant access to information pushes technology even further, the eventual integration of these technologies into our everyday lives may cause some people to ask if we pushed too hard, too far and too fast. Prompting the debate, should controls be designed concurrent with the technology or do the exposures as a result of the technology, then drive the design of the needed controls?

Google's $3.2 billion acquisition of Nest (www.nest.com) could be a good start to that debate. If you haven't heard of it, you will more and more as we move into the second decade of the 21st century, the "Internet of Things" (IoT, for short). IoT, is a phrase for when everyday objects are connected to the Internet and participating together on a system, although it also means the convergence of conventional connected devices and smart appliances?.

The goal of IoT is to have people seamlessly retrieve knowledge and function on a day-to-day basis without having to sit down at a computer or talk to another human. It's like ubiquitous computing,

but it goes beyond Google Glass and extends to every home, car, business, building, and system in the world.[ii]

The Nest Learning Thermostat is an IoT. It learns your schedule, programs itself, and can be controlled from your phone. Most people leave the house at one temperature and forget to change it. So, on the surface it sounds like a good thing.

Nest's Learning Thermostat will ask for or obtain the following information upon installation and during usage:

- If Nest is located in a home or business.
- Where in your home you are installing the device.
- Your postal or zip code.
- Operational information pulled directly from your heating and cooling (HVAC) system to learn its capabilities.
- Current temperature, humidity, and ambient light in the room.
- Whether something in the room is moving (e.g., intruders as well as allowing for the detection of smoke and CO_2 in your home).
- Any temperature adjustments detected by the device.
- Heating and cooling information.
- A record of every time your system turns on and off.
- Nest model and serial number, software version, and technical information such as battery charge level.

To access your Nest Product over the Internet from a computer, a smartphone, or a tablet:

- You will need to connect it to your Wi-Fi network
- Provide your Wi-Fi network name (SSID) and password

Taking a quick look at the types of data that can be collected about an individual's personal living habits by just this one Internet-connected device raises questions regarding the potential disclosure, sale (read intra-, external-company transfer), or court-ordered release of data to such entities as:

- State agencies looking to validate individual homeowner claims for energy tax credit rebates.
- Manufacturers wishing to substantiate claims to heat/cooling cost reductions of their products.
- Vendors selling home energy evaluation services aimed at reducing a homeowner's energy bill.
- Duct cleaning companies claiming that an annual cleaning will lower energy costs, again based on data regarding the homeowner's energy "read out."
- Divorce attorneys looking to make a case for poor parental care of a child (or children) because the average daily heat in the house was kept below "x" degrees during the last "n" number of coldest winter days. The reverse claim as to AC levels during the heat of the summer.
- Insurance companies who may deny a homeowner's claim for water damage from burst pipes due to the extreme winter temps, stating that the homeowner failed to keep the temperature in the house at an appropriate level to prevent such damage, thus not taking proactive care to prevent such damage in the first place.
- Power companies charging premiums to customers based on an individual customer's power usage (read lack of "good" power

conservation habits) or discounts based on verifiable "good" power conservation habits.
- Various companies selling everything under the sun designed to eke out better energy savings and performance from an individual's home (think solar blankets, roof fans, window sun shades, landscaping system, pipe wrapping, window replacement, roof replacements, etc.).

Who is protecting your personal, private information? Nest? Google? You?

After synching your mobile device to your home thermostat and leaving for the office or turning on your home security system before drifting off to sleep, do you wonder exactly what your multi interconnected, third-party serviced home really knows about your private life, your activities, and personal habits?

Walls, people have said in hushed voices, have ears! Now they have better ears (audio sensors), eyes (camera/video sensors), noses (smoke and carbon dioxide sensors), and touch (room or body temperature variance detectors) capabilities. Scary thoughts when one comes to expect the privacy and sanctity of one's castle.

Have you asked yourself who has access to all of these data and what are they doing with it? Have you asked your alarm service provider? Your power company? Google? What response did you receive? Were you comfortable, satisfied with that response?

The world is in the midst of a dramatic transformation from isolated systems to Internet-enabled devices that can network and communicate with each other and the cloud.

The enormous volumes of data generated and shared across intelligent devices and systems can now be analyzed, and the untapped value extracted to serve the business. This enables companies to provide better products and services enabling new business models and enriched consumer experiences.[iii]

"'Open the pod bay doors, HAL.'
'I'm sorry, Dave. I'm afraid I can't do that.'"
◆ *2001: A Space Odyssey (1968 film)*

THE PRIVACY AUDIT: MITIGATING PERSONAL RISKS

Many of us have performed or participated in a privacy audit, conducted on behalf of our clients or for our company. When was the last time you performed a personal privacy audit? Maybe it's time!

Just as we would perform a privacy audit for a client or of a corporation, asking similar questions regarding our personal privacy may help to identify exposure areas requiring prompt attention to mitigating risks and the possible misuse and loss of PII.

Performing a personal privacy audit should focus on determining the control over personal information that can be linked to or used to identify you either directly or indirectly such as:

- Name
- Home or e-mail address
- Social Security, passport, or account numbers
- Physical characteristics
- Credit records
- Consumer purchase history
- Employee files

Control over sensitive personal information such as: medical records; financial information; political opinions; religious or philosophical beliefs; and so on should also be included in such an audit.

How would you answer the following questions regarding your personal privacy?

1. Is the use of your PII and private, personal information, provided to or obtained by, third-party service providers in fulfillment of service requirements on your behalf, controlled from unauthorized use and access?
2. Is your PII and private, personal information used only for necessary and lawful purposes?
3. Are you able to verify that your private, personal information collected for a particular purpose is not used for another purpose without your explicit consent (unless such collection and use is specifically authorized or mandated by law)?
4. Have you exercised your "opt-out" rights by declining to provide personal information or by consenting only to a particular use (e.g., allowing basic use of your personal information, but not sharing with other third-parties) on all sites, with all third-party service providers/vendors where applicable?

   A business is required to notify you of its existing policies that allow you to choose to share your information (opt-in) or that allow you to stop the sharing of your information (opt-out) for marketing purposes. If the company has such a policy, then it must provide you with a free method to opt-in or opt-out.

   Businesses that consistently maintain opt-in or opt-out policies are exempt from the disclosure requirements. If a company has given you the opportunity to opt-out and you decline, you will be unable to discover which additional companies may have received your personal information.

   If you feel you were harmed because a company did not disclose this information as required, you can file a civil lawsuit to recover damages. Damages are limited to $500. If the court finds the violation willful, intentional, or reckless, you can recover up to $3,000. This situation might arise if a company refuses to track how information is shared or has been repeatedly fined $500 and is making no effort to comply with the law. The plaintiff is also entitled to reasonable attorney fees and expenses.

   If the violation is not willful, intentional, or reckless, the law gives companies a 90-day grace period. A business will not have to pay the $500 if it provides the information within 90 days of notification of failure to comply with the law.[iv]
5. Who will have access to your collected data (e.g., employees, managers, system administrators, developers, contractors, others)?
6. Have you been provided with an explanation for their purpose for having access to this information?
7. How is access to your collected data determined?
8. Will third-party employees have access to all data acquired and stored on the third-party's system or will the employee's access be restricted?

9. What controls are in place to mitigate the misuse (e.g., browsing) of data by those having access?
10. Who is responsible for assuring proper use of these data?
11. How will data collected be checked for completeness? Accuracy?

Would you successfully pass a personal privacy audit? What outstanding audit items need immediate remediation? Where do your personal risks lay due to inadequate controls over your personal privacy? Something to keep in mind about giving out your personal information: If you are not paying for something when you give this information away that makes you the product being sold. In that light, how well do you know those organizations you just gave your information to?

"When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else."
◆ *David Brin*

PROTECT THYSELF

Technology provides us with a multitude of options for limiting our exposure and protecting our personal privacy. Given the rapid deployment of mobile technologies, the number and availability of diverse devices and the global consumer dependency on e-mail, text messaging, online chats, and voice mail, a good first step is to evaluate the security of your data sent, accessed and shared via these devices.

There are many tools available designed to protect your personal (and presumably) private communications. These are tools that empower you to opt-out from the surveillance-by-default communications channels most of us use, and instead keep your private thoughts and words, exactly that—private.

For private voice communications there is Jitsi (Jitsi .org) an audio/video Internet phone and instant messenger written in Java. Jitsi supports some of the most popular instant messaging and telephony protocols such as SIP, Jabber/XMPP (and hence Facebook and Google Talk), AIM, ICQ, MSN, Yahoo! Messenger. Jitsi offers privacy and encryption for calls as it incorporates Zfone's ZRTP encryption protocol.

The encryption software Zfone (www.zfone.com) makes it impossible for eavesdroppers to listen in on Voice-over-Internet-protocol (VoIP) phone calls. Zfone issues encryption keys that bypass the servers routing Internet calls and sets up the encryption directly on the voice channel. That added layer of protection means even if someone can access the server that routes a call, there's no way to decrypt the call's contents.[v]

For private voice calls on mobile devices Cellcrypt (www.cellcrypt.com) and ChatSecure (www.hatsecure.org), encrypt voice calls that makes secure calling as simple as making a normal call.

Looking for added privacy for your text and chat messaging? Check out Off-the-Record (OTR) technologies like, OTR Messaging, which allows you to have private conversations over instant messaging by providing:

- Encryption—No one else can read your instant messages.
- Authentication—You are assured the correspondent is who you think it is.

- Deniability—The messages you send do not have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, during a conversation, your correspondent is assured the messages he sees are authentic and unmodified.
- Perfect forward secrecy—If you lose control of your private keys, no previous conversation is compromised.[vi]

"I will not be pushed, filed, stamped, indexed, briefed, debriefed, or numbered. My life is my own."
◆ *The Prisoner (Patrick McGoohan—Number Six)*

Need real anonymity? Download the Tor Browser Bundle (www.torproject.org). Tor has become famous as a secure way for activists, journalists, and, yes, some criminals, to browse the Web. Tor bundles your data into encrypted packets and directs it through a worldwide volunteer network of more than 3,000 servers, hiding your location and making your data more difficult to read along the way.[vii] (See Table 1 for additional personal privacy software.)

There exists a multitude of ways, with new ways emerging daily, to protect your privacy and to mitigate the risks of unauthorized access and disclosure of your private information. However, failing to take the necessary steps to identify and implement these controls is no longer (it has never really been) an option.

CONCLUSION

In the long run, the best approach to mitigating the loss of privacy (personal or corporate) is through ongoing, proactive education and vigilance.

Maintaining an ongoing awareness of current and emerging technologies and exploits designed to relieve you of private, confidential data is the best approach for protection. Perform regular, real-time reviews of purchases and financial statements for anomalies. Learn to recognize and avoid scams, cons, and exploits designed

Table 1 ***Selected Personal Privacy Software***

BetterPrivacy	https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/
buddycloud	http://buddycloud.com
Dashlane	https://www.dashlane.com/passwordmanager
Delete Me	www.abine.com/deleteme/landing.php
Disconnect	https://disconnect.me
Ghostery	https://www.ghostery.com/en
HTTPS Everywhere	https://www.eff.org/https-everywhere
ixquick	https://ixquick.com/
KoolSpan	www.koolspan.com
LastPass	https://lastpass.com
Neomailbox	https://www.neomailbox.com
Off-the-Record Messaging	https://otr.cypherpunks.ca
Orbot	https://guardianproject.info/apps/orbot
P.G.P (Pretty Good Privacy)	www.pgpi.org
RedPhone: Secure Calls	https://whispersystems.org
RoboForm	www.roboform.com
Silent Circle	https://silentcircle.com/
SpiderOak	https://spideroak.com
TextSecure Private Messenger	https://play.google.com/store/apps/details?id=org
Tor browser	www.torproject.org
TrueCrypt	http://www.truecrypt.org

Table 2 ***Privacy Resources***

Resource	URL
American Civil Liberties Union	www.aclu.org
Australia Office of the Privacy Commissioner	www.privacy.gov.au
Canadian Office of the Privacy Commissioner	www.priv.gc.ca
Center for Democracy and Technology	www.cdt.org
Center for Digital Democracy	www.democraticmedia.org
Coalition Against Unsolicited Commercial Email (CAUCE)	www.cauce.org
Computer Professionals for Social Responsibility	http://cpsr.org
Consumer Project on Technology (CPT)	www.cptech.org
Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)	www.nocards.org
Cyber-Rights & Cyber-Liberties (UK)	www.cyber-rights.org
Electronic Frontier Foundation (EFF)	www.eff.org
Electronic Privacy Information Center (EPIC)	http://epic.org
Enterprise Privacy Authorization Language (EPAL)	www.w3.org/Submission/2003/SUBM-EPAL-20031110/
Federal Trade Commission	www.ftc.gov
Global Internet Liberty Campaign	http://gilc.org
Network Advertising Initiative (NAI)	www.networkadvertising.org
Privacy and American Business	www.pandab.org
Privacy Coalition	http://privacycoalition.org
Privacy Exchange	www.privacyexchange.org/
Privacy Foundation	www.law.du.edu/index.php/privacy-foundation
Privacy International	www.privacyinternational.org
Privacy Journal	www.privacyjournal.net
Privacy Law in the USA	www.rbs2.com/privacy.htm
Privacy Laws & Business	www.privacylaws.com
Privacy Rights Clearinghouse	www.privacyrights.org
Privacy Times	www.privacytimes.com
Privacy.net	http://privacy.net
Privacy.org	http://privacy.org
Private Citizen	www.private-citizen.com
Tech Law Journal	www.techlawjournal.com
The International Association of Privacy Professionals	www.privacyassociation.org
The Platform for Privacy Preferences Project (P3P)	www.w3.org/P3P/
US Dept. of Health & Human Services IT	http://www.healthit.gov
US Public Interest Research Group (PIRG)	www.uspirg.org

to probe and gather your personal, private information. Evaluate technology, assess exposures to your personal information, and implement those technologies (think mobile apps) that you have vetted and trust. Routinely perform personal privacy audits and respond immediately to identify exposures, weaknesses and gaps.

Have ongoing discussions with children and seniors on the dangers and risks of disclosing not only PII but any personal, private information. Emphasize to always first verify and validate the authentication of an individual requesting any personal information and then, the specific need and authorization for the collection of any personal data, prior to releasing these data. (See Table 2 for additional privacy resources.)

As for cameras in the neighborhood: "When you weigh cameras against other security measures, they emerge as the least costly and most effective choice. In the aftermath of 9/11, we've turned most public spaces into fortresses—now, it's impossible for you to get into tall buildings, airports, many museums, concerts, and even public celebrations without being subjected to pat-downs and metal detectors. When combined with competent law enforcement, surveillance

cameras are more effective, less intrusive, less psychologically draining, and much more pleasant than these alternatives."[viii]

Although this may be a logical analysis, it still begs the question . . . given the ever increasing and evolving sophistication of technology and the integration of these technologies into our daily, personal lives, exactly how comfortable are you with the erosion of your privacy as payment for your security?

To put it in a different light, how could that neighborhood camera information be used against you? Is it worth the risk or price of your physical safety?

The latter question will be explored in the third installment of this series, corporate versus personal security and privacy. Who really owns your data?

"They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."
◆ *Ben Franklin*

Notes

i. World Population Clock as of March 17, 2014 at 10:06 CDT, www.census.gov/popclock (retrieved March 2014).
ii. Betters, E. (January 15, 2014). "Internet of Things Explained: What is It, and Can It Really Change the World?" www.pocket-lint.com/news/126559-internet-of-things-explained-what-is-it-and-can-it-really-change-the-world (retrieved February 2014).
iii. Intel, "The Internet of Things Starts with Intelligence Inside," www.intel.com/content/www/us/en/intelligent-systems/iot/internet-of-things-starts-with-intelligence-inside.html (retrieved February 2014).
iv. "'Shine the Light' on Marketers: Find out How They Know Your Name." (November 2013). Privacy Rights Clearinghouse, www.privacyrights.org/shine-light-marketers-find-out-how-they-know-your-name#8 (retrieved March 2014).
v. Greene, K. "Encryption Software May Halt Wire Tapping," http://m.technologyreview.com/read_article.aspx?id=16948&ch=infotech (retrieved February 2014).
vi. Off-the-Record (OTR) Messaging, https://otr.cypherpunks.ca/index.php#docs (retrieved February 2014).
vii. Alba, D. (February 4, 2014). "7 Ways to Reclaim Your Digital Privacy," www.popularmechanics.com/technology/how-to/computer-security/7-ways-to-reclaim-your-digital-privacy-16453529 (retrieved March 2014).
viii. Manjoo, F. (April 18, 2013). "We Need More Cameras, and We Need Them Now, the Case for Surveillance," Slate, www.slate.com/articles/technology/technology/2013/04/boston_bomber_photos_the_marathon_bombing_shows_that_we_need_more_security.html (retrieved February 2014).

Albert J. Marcella Jr., Ph.D., CISA, CISM, is president of Business Automation Consultants, LLC. Dr. Marcella, is an internationally recognized public speaker, researcher, and workshop and seminar leader with over 35 years of experience in IT audit, security, and assessing internal controls. Dr. Marcella, has authored numerous articles and 29 books on various IT, audit, and security related subjects.

Carol Stucki, CISA, PMP, is a Project Manager with over 25 years of experience in operational and IT roles including providing internal systems consulting, portfolio management, and auditing services for companies both in the Unites States and abroad. Carol has worked for GTE (now Verizon), Arthur Andersen, Perot Systems, Los Alamos National Labs on DOE, DOD, HSD contracts, Church of Jesus Christ of Latter-day Saints, Capgemini, and HealthNow.

EDPACS
THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

2014 VOL. 50, NO. 3

PRIVACY AND SECURITY PART III: WORLDS IN COLLISION

AL MARCELLA AND CAROL STUCKI

Abstract. This article is the third and final in a series that explores the issues of privacy versus security. The first article, "Privacy and Security Part I: Privacy and Security in the Corporate World" covered the corporate side. The second article, "Privacy and Security Part II: It's Personal" explored personal privacy versus security. This third installment will review the overlap from both sides corporate versus personal privacy: Who really owns your data?

THE PAST IS NOT MUCH DIFFERENT FROM THE PRESENT

Whether lines from Henry James's 1888 novel *The Reverberator*, *"If these people had done bad things they ought to be ashamed of themselves and he couldn't pity them, and if they hadn't done them there was no need of making such a rumpus about other people knowing"* or from Ashton Kutcher, *"I think privacy is valuable. ...But at the end of the day, if you're not doing anything wrong, you don't have anything to hide." "Do you really have nothing to fear?"* it is clear that privacy and the expectation of same, remains an important social issue. Such concern for one's personal privacy and how that privacy will be both assured and protected, will certainly not diminish over time.

In an era of social media, big data, National Security Agency (NSA) clandestine programs, the growing emergence of the IoT (Internet of Things), data breeches, hackers in your Heating, Ventilation, and Air Conditioning (HVAC) system, malware-infected online takeout menus, and just in time for summer, when you thought it was safe to go back into the water... Six Flags announces that your fingerprints will be required to enter their theme parks;

It was a bit of a shock to Jason Kirkpatrick, 38, of south St. Louis County, who visited the park (Six Flags Saint Louis) with his 3-year-old son and 5-year-old daughter this past weekend. He had to pick his son up so the machine could scan his finger.

IN THIS ISSUE

- **Privacy and Security Part III: Worlds in Collision**
- **Demystifying Disclosure Controls: Understanding Them to Effectively Leverage Toward Objectives**

It was tough for him to pinpoint exactly what bothered him. Maybe it was just one more sign of the erosion of privacy in modern society. Maybe it was where the information could eventually end up. Maybe both.

"You don't know what they can do with it. Or more importantly what someone else could do with it," he said. "It just feels more personal than a photo."[1]

"Privacy and security are those things you give up when you show the world what makes you extraordinary."
◆ *Margaret Cho*

What is happening to the sanctity of individual privacy? To what lengths does an organization need to go to protect its data assets, infrastructure, employees, and customers? How capable is your organization in balancing security with the protection of individual privacy?

Is your organization prepared to address the ramifications arising from the failure to protect private information? What is your organization's privacy protection strategy? Does the organization know what its privacy history has been, where it is currently in the capability and ability to protect and secure private information and does it know where it is headed?

Drawing a blank stare or a non-response from corporate management may be indicative of deeper troubles and more problems to come. Not currently under investigation, party to a lawsuit . . . it may not be a matter of *if* but, *when*.

These issues where the focus of the preceding two articles in this series.

This final installment examines issues, raises concerns, and asks questions as an inevitable result of the collision between the worlds of privacy and security.

The necessity for strong security and strong privacy seem destined to collide and stuck in the middle, data. No, not Brent Spiner, Lieutenant Commander Data in *Star Trek: The Next Generation* (for those readers who demand and rightfully so, accuracy in all things Star Trek) but data of all imaginable types and sources, ultimately to be turned into information that propels life as we know it today and drives global economies.

SLOW EROSION OF PRIVACY IN THE NAME OF SECURITY

An examination of the U.S. Constitution reveals not a single word related to a citizen's right to privacy. Bottom line, citizens have none (privacy that is), at least not constitutionally guaranteed and

Table 1 ***U.S. Legislation—Privacy Protection for U.S. Citizens***

Privacy of Communications
Telephone Consumer Protection Act of 1991
Children's Privacy
Children's Online Privacy Protection Act (COPPA) of 1998
Privacy of Financial Information
Fair Credit Reporting Act (1970)
Right to Financial Privacy Act (1978)
Fair and Accurate Credit Transactions Act (2003)
Privacy of Government Collections
Census Confidentiality Statute of 1954
Freedom of Information Act (1966)
Privacy Act of 1974
Privacy of Medical Records
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Privacy of Miscellaneous Records and Activities
Family Education Rights and Privacy Act [FERPA] (1974)
Privacy Protection Act of 1980
Cable Communications Policy Act of 1984
Video Privacy Protection Act of 1988
Employee Polygraph Protection Act of 1988
Driver's Privacy Protection Act of 1994
Do-Not-Call Implementation Act of 2003

at least not in the United States (we as U.S. citizens lag significantly behind many developed nations in acquiring this particular "right").

How then are personal privacy rights protected and respected? A quick review of the U.S. Constitution shines some light on the government's role in attempting to protect citizen's right to privacy. For example:

1st Amendment: Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

4th Amendment: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. The 4th Amendment protects U.S. citizens against unreasonable search and seizure.

For additional examples of legislation designed to protect individual privacy see Table 1.

These amendments are broad reaches and yet do not address many of the details of an individual citizen's daily privacy concerns. Governmental and administrative reach between the worlds of privacy and security can be seen in the conflict arising between privacy and national security.

The linkage of personal privacy and stronger security, even in the face of protecting national security, can clearly be seen in the progression of U.S. legislation such as:

The Foreign Intelligence Surveillance Act (FISA) of 1978. As a result of a Freedom of Information Act (FOIA) lawsuit, the Electronic Privacy Information Center obtained copies of the Attorney General Reports on the government's electronic surveillance activities. These reports have been submitted to Congress every six months since 2001 but have never before been disclosed to the public. These reports include new details about government collection of telephone and Internet records. The reports include the number of U.S. persons targeted for "Pen Register" surveillance under the Foreign Intelligence Surveillance Act.[ii]

Semiannual Report of the Attorney General on Electronic Surveillance and Physical Search under the Foreign Intelligence Surveillance Act, filed June 2013, reported that between July 1 and December 31, 2012, the Government filed 69 applications with the [Foreign Intelligence Service Court] FISC seeking authorization for the FBI to conduct PRITT surveillance pursuant to 50 U.S.C. ÏÏ 1841–1846, as amended. The FISC approved all 69 PRITT applications filed during the reporting period. In these 69 applications, 32 named U.S. persons were the targets of PRITT surveillance. The FISC did not deny in whole or in part, any FBI PRITT applications during this reporting period.[iii]

Executive Order 12333 of 1981 [As Amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)]. Part 2 Conduct of Intelligence Activities. Accurate and timely information about the capabilities, intentions, and activities of foreign powers, organizations, or persons and their agents is essential to informed decision making in the areas of national defense and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.[iv]

The Computer Security Act of 1987. The U.S. Congress declared that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby created a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

National Security Directive (NSD) 42 of 1990. The roles and responsibilities for securing national security systems are established by National Security Directive 42 (NSD-42). NSD-42 establishes what is now called the Committee on National Security Systems, which it authorizes to develop, and require compliance with, standards and guidelines for national security systems.

The Health Insurance Portability and Accountability Act of 1996 (P.L. 104–191, Title II, Subtitle F, Sec. 262, 42 USC 1320d et seq.) authorizes the Secretary of Health and Human Services to adopt standards that require health plans, health care providers, and

health care clearinghouses to take reasonable and appropriate administrative, technical, and physical safeguards to: ensure the integrity and confidentiality of individually identifiable health information held or transferred by them; to protect against any reasonably anticipated threats, unauthorized use or disclosure; and to ensure compliance with these safeguards by officers and employees.[v]

Title V of the Gramm-Leach-Bliley Act of 1999 (P.L. 106-102, 15 USC Chpt. 94, Ï6801 et seq.) requires financial institutions to protect the security and confidentiality of their customers' non-public personal information.

USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) of 2001. Focuses mainly on reinforcing the arsenal of tools available to the Central Intelligence Agency, the Federal Bureau of Investigation, and federal prosecutors for identifying and disabling terrorist networks operating both within and outside the United States. Summary of key sections of the USA Patriot Act related to privacy include:

Title II—Enhanced Surveillance Procedures

- Section 209: Allows law enforcement to seize voice mail messages pursuant to a warrant.
- Section 210: Allows law enforcement to subpoena additional subscriber records from service providers such as "records of sessions and durations" and "means and source of payment."
- Section 220: Allows for "Nation Wide Service of Search Warrant for Electronic Evidence."

Title V—Removing Obstacles to Investigating Terrorism

- Section 505: Allows law enforcement easier access to telephone toll and transactional records, financial records, and consumer reports.[vi]

"The U.S. Constitution protects our privacy from the prying eyes of government. It does not, however, protect us from the prying eyes of companies and corporations."
◆ *Simon Sinek*

Yet, even with the force of legislation, protecting and securing one's individual privacy is becoming increasingly more difficult and challenging. Global economies fueled by technology and increasingly consuming record amounts of data annually, places an enormous value on that commodity and subsequently the information represented within those data.

Does your organization have in place procedures that address the legal request for the wholesale delivery of data belonging to clients, employees, trading partners? Would such a request and your required compliance negate your privacy policy, alienate customers, affect investors? What legal rights does you organization have to refuse such requests? Is your organization prepared to communicate your compliance and delivery of requested data to its clients, trading partners, stakeholders, and so on?

What is at risk when the line is crossed, when boundaries between privacy and security become blurred? With so much data and associated, valuable information that can be gleaned from those data, even unintentional, legally required data gathering, may violate or jeopardize one's privacy.

When technology is exploited, ultimately it is individuals who are placed at risk.

PRIVACY LOST

It may be possible to legislate Big Brother but, doing the same to big business is quite a different story.

What are the threats to personal privacy when such threats are downplayed in the name of safety or security? Most readers would probably opt for stronger security, better safety but, with the proviso that consent be obtained prior to disclosing or relinquishing private, personal data. Additionally, knowing exactly what data are being recorded, collected, assembled and how these data are to be used when disclosed, relinquished or shared with external third-parties.

Let's look at a few examples from our daily lives where technology and the ability to synthesize billions of bits of data into information can potentially lead to the further erosion of one's personal privacy.

Automobiles are integrating computing technology that enhance the ability of others to collect location and operation data in near real time. In our data driven economy this data has value. Transportation technology is rapidly emerging and converging, blurring the lines between safety and security and that of personal privacy.

Take for example the engine control unit (ECU), which is the most powerful computer on most cars. The ECU knows the coolant temperature, amount of oxygen in the exhaust, and engine speed. The transmission controller knows the vehicle speed. The controller for the anti-lock braking system (ABS) knows if there is a problem with the ABS.[vii]

Other information available from your auto's in-board computing and diagnosis systems includes but is not limited to:

- Engine and car speed
- Miles driven
- Last service date
- Fuel consumption (which *can help determine driving habits*)
- Air bag use
- Weight in passenger seats

This information accessed by the auto manufacture under a warranty claim may be used to show owner failure to properly care for the vehicle (missing required or recommended service dates, oil changes, etc.), excessive speeds above locally posted limits, hard braking, any of which may have contributed to vehicle failure and all controlled by the vehicle's owner and no fault of the manufacturer.

Weight in passenger seats? Wow, could your auto communicate this to your Garmin, TomTom, or Magellan, and override directions to the nearest fast food chain and instead offer words of encouragement through the audio system and send you instead to a salad and wraps restaurant?

If the weight recorded is under a predetermined weight, the sensor may determine that a minor may be sitting in the driver's seat and opt to override the auto ignition command and not start the car, preventing a possible accident when keys are mistakenly left in the ignition and a child attempts to start the car.

The event data recorder (EDR), more commonly known as the *black box*, is installed in 96 percent of all new vehicles sold in the United States. As of model year 2013, all EDRs must record:

- Change in forward crash speed
- Maximum change in forward crash speed
- Time from beginning of crash at which the maximum change in forward crash speed occurs
- Speed vehicle was traveling
- Percentage of engine throttle, percentage full (how far the accelerator pedal was pressed)
- Whether or not brake was applied
- Ignition cycle (number of power cycles applied to the EDR) at the time of the crash
- Ignition cycle (number of power cycles applied to the EDR) when the EDR data were downloaded
- Whether or not driver was using safety belt
- Whether or not frontal airbag warning lamp was on
- Driver frontal airbag deployment: time to deploy for a single stage airbag, or time to first stage deployment for a multistage airbag
- Right front passenger frontal airbag deployment: time to deploy for a single stage airbag, or time to first stage deployment for a multistage airbag
- Number of crash events
- Time between first two crash events, if applicable
- Whether or not EDR completed recording
- Sideways acceleration
- Forward or rearward acceleration
- Engine speed
- Driver steering input
- Right front passenger safety belt status
- Engagement of electronic stability control system
- Antilock brake activity
- Side airbag deployment time for driver and right front passenger
- Seat track positions for both the driver and right front passenger
- Occupant size and position for drivers and right front passengers[viii]

"The pace of development of sensors is moving much faster than folks can keep up with."
◆ *Ted Colbert, CIO, Boeing*

EDRs can be used to corroborate findings from traditional crash investigation techniques, but they can also provide information about a crash that can't be obtained through traditional methods. Police, crash investigators, automakers, insurance adjusters and highway safety researchers can use this information to analyze what occurred leading up to and during a crash.

For crashes that do not involve litigation, especially when police or insurers are interested in assessing fault, insurers may be able to access the EDRs in their policyholders' vehicles based on provisions in the insurance contract requiring policyholders to cooperate with the insurer.[ix]

The emergence of technology-driven autos raises the question who owns your car's data? You? The finance company? Bank? Insurance company? Law enforcement?

Senate Bill S. 1925, to limit the retrieval of data from vehicle event data recorders, the Driver Privacy Act, passed in January 2014, answers the question, "who owns the data?" You do, the

car's owner, although you may be required to consent to providing access to these data by law enforcement, accident investigators, and/or your insurance company.

Have you really read your auto insurance policy? Do you know your rights to refuse consenting to access the EDR in your auto?

And that was just in your car. There are other sensors in your life. Under the rapidly growing category of IoT (Internet of Things) the possibility of losing one's privacy is increasing at a rate that may be impossible to control.

The IoT is set to explode, driven largely by the consumer market, where the number of smart "things" and everyday products equipped with IP-addressable sensors—from wearable smart bands to smart refrigerators—is multiplying exponentially. Research firm Gartner estimates that 26 billion IoT-ready products will be in service by 2020. That's an average of 3.3 devices for every man, woman, and child on the planet. And that does not include the projected 7.3 billion smartphones and tablets.[x]

The IoT is a scenario in which objects, animals, or people are provided with unique identifiers and the ability to automatically transfer data over a network without requiring human-to-human or human-to-computer interaction. Any natural or man-made object that can be assigned an IP address can be provided with the ability to transfer data over a network.[xi]

Advanced metering systems are comprised of state-of-the-art electronic/digital hardware and software, which combine interval data measurement with continuously available remote communications. These systems enable measurement of detailed, time-based information and frequent collection and transmittal of such information to various parties.

Advanced Metering Infrastructure (AMI) typically refers to the full measurement and collection system that includes meters at the customer site, communication networks between the customer and a service provider, such as an electric, gas, or water utility, and data reception and management systems that make the information available to the service provider.

IoT coupled with AMI provides a richness of data not previously seen nor accounted for and raises concern when questioning the controls and usage of those data generated and available through the union of IoT and AMI.

What risks will there be to one's personal privacy, when data from advanced metering systems linked with IoT-enabled devices, can communicate with a host of external third-parties and share (or sell) specific end user/consumer/citizen data?

Take a look for example at products such as ZigBee, Z-Wave, and Nest, technology products designed to provide direct consumer control over energy utilization within private homes and commercial buildings, leading eventually to a reduction in energy costs. ZigBee and other networks provide smart, low-cost, low-power, low-maintenance monitoring and control systems; in effect, a smart meter, used to tie an entire home, office, or factory together for safety, security, and control.

Such AMI-based, smart meter devices can:

- Monitor power use
- Turn on/off devices remotely

- Easily add devices to create an integrated smart home security system
- Customize lighting levels based on activity and create scenes
- Control of plug-in hybrid electric vehicles (PHEVs) charging

Smart meter nodes are embedded in hundreds of sensors and controls that are built into large infrastructures for home automation, industrial automation, remote metering, automotives, medical equipment, patient monitoring, asset tracking systems, security systems, lighting and temperature control systems, and even toys.[xii]

In order to collate and analyze data to produce patterns of use, efficiency levels and peak/off peak times, the technology is able to track when an energy user is at home, and more, such as when you:

- Go to work
- Wake up
- Come home
- Watch TV
- Go on vacation
- Take a hot bath
- Cook meals (e.g., patterns and times)
- Play a computer game
- Surf the Web

All these data points and more can be tracked through the use of electricity and gas and recorded by the smart meter.

The downside is that with the data gathered by ZigBee-like devices, other people and businesses can also become more aware of your habits. For example:

- Divorce attorneys looking to make a case for poor parental care of a child (or children) because the average daily heat in the house was kept below "x" degrees during the last "n" number of coldest winter days. The reverse claim as to AC levels during the heat of the summer.
- Insurance companies who may deny a homeowner's claim for water damage from burst pipes due to the extreme winter temps, stating that the homeowner failed to keep the temperature in the house at an appropriate level to prevent such damage, thus not taking proactive care to prevent such damage in the first place.
- Power companies charging premiums to customers based on an individual customer's power usage (read lack of "good" power conservation habits) or discounts based on verifiable "good" power conservation habits.

The commercial value of information detailing the lifestyle and habits of a consumer is high— and it is not only utility companies that are interested. Marketing firms could use this valuable data, and potentially criminals may be able to use the information to find out when consumers are not at home.[xiii]

Bottom line, is the potential energy savings worth the invasion of privacy?

Not quite yet but, you know it's coming. . .

With the proliferation of the "Internet of Things" the ability of the embedded technology in your "smart" refrigerator to read the UPC codes on the refrigerator's contents and communicate that list

to your insurance provider, who then determines that you are not eating or living a healthy lifestyle and automatically raises your next quarter's life insurance premium.

Or better yet, threatens to do so unless you enroll in some sort of "healthy lifestyle coaching class," naturally sponsored or run by the insurance provider's wholly owned third-party subsidiary. Your refrigerator sends monthly reports on its contents to your insurance provider as a result of your failing the healthy foods and lifestyle "audit."

Interested in rock or ice climbing, kayaking, parasailing, riding a bike through Provence this summer, and you have searched for or even purchased books or tour guides from your favorite online book seller?

The online retailer makes this information available to your insurance carrier and you receive a notice indicating that your current life insurance policy does not cover these types of riskier activities and offers you a fix-term, high-risk activity rider (for a substantial fee of course) to be added to your current life insurance policy to cover perceived high risk activities.

You are also duly notified that if you engage in any of these activities without said rider, now having been appropriately notified, your life insurance policy may be cancelled (with a forfeiture of paid-in premiums no less).

No way, don't think so, can't happen. . .just wait, in some cases, its already happened.

"Policy makers need to provide the institutional framework to allow companies to easily create value out of data while protecting the privacy of citizens and providing data security." ◆ *McKinsey Global Institute report,* Big data: The next frontier for innovation, competition, and productivity

DATA IDENTIFIERS AND THE RISK TO PERSONAL PRIVACY

Datasets containing micro-data, that is, information about specific individuals, are increasingly becoming public in response to "open government" laws and to support data mining research. Some datasets include legally protected information such as health histories; others contain individual preferences and transactions, which many people may view as private or sensitive.[xiv]

As an ever larger amount of data is digitized and travels across organizational boundaries, there is a set of policy issues that will become increasingly important, including, but not limited to, privacy, security, intellectual property, and liability. Clearly, privacy is an issue whose importance, particularly to consumers, is growing as the value of big data becomes more apparent.[xv]

With the availability of so much data, gleaned from so many collection devices, the lack of properly assessing, validating, controlling, and managing these data will inevitability place individuals at risk and certainly further strip away the last vestiges of one's privacy.

One result of the availability of access to billions of data identifiers and the technology to comb through these data, is the ability to associate a particular behavior or pattern with a specific data owner or group of data owners.

A user profile is a collection of information that describes the various attributes of a user. These attributes may include geographical location, academic and professional background, membership in groups, interests, preferences, opinions, and so on. User

Table 2 ***Methods for Obtaining User Profiles****

Profile method	Description
Explicit Information	The simplest way of obtaining information about users is through the data they input via forms or other user interfaces provided for this purpose. Generally, the information gathered in this way is demographic, such as the user's age, gender, job, birthday, marital status, and hobbies.
Observation of a User's Actions	The most widely used method for obtaining information about users is observing their actions with the underlying application, recording or logging these actions, and discovering patterns from these logs through some Machine Learning or Data Mining technique.
User Feedback	User feedback is a key source of learning in interface agent technology. This feedback may be explicit, when users explicitly evaluate an agent's actions through a user interface provided for that purpose, or implicit, when the agent observes a user's actions after assisting him to detect some implicit evaluation of its assistance.
Stereotypes	A stereotype is the representation of relevant common characteristics of users pertaining to specific user subgroups of an application system.
Intelligent User Profiling Techniques	Intelligent user profiling implies the application of intelligent techniques, coming from the areas of Machine Learning, Data Mining or Information Retrieval, for example, to build user profiles.
1. Bayesian Networks	A Bayesian network (BN) is a compact, expressive representation of uncertain relationships among variables of interest in a domain.
2. Association Rules	Association rules are a data mining technique widely used to discover patterns from data. They have also been used to learn user profiles in different areas, mainly in those related to e-commerce and web usage.
3. Case-Based Reasoning	CBR is a technique that solves new problems by remembering previous similar experiences. CBR has been used to build user profiles in areas like information retrieval and information filtering.

*Schiaffino, S., and A. Amandi (2009). "Intelligent user profiling," in *Artificial Intelligence an International Perspective*. Springer, pp. 193–216, www.exa.unicen.edu.ar/catedras/knowmanage/apuntes/56400193.pdf (retrieved April 2014).

profiling is the process of collecting information about a user in order to construct their user profile. User profiling raises a significant threat to user privacy.

One can assume that an ethical and trustworthy service would use the information collected in a user profile with the user's explicit consent and only for the benefit of the user. However, services that are less inclined toward protecting user privacy, may use user profiles for a number of purposes which may not be approved by the user (see Table 2) and which may result in disclosure of personal information.[xvi]

As demonstrated by Narayanan and Shmatikov, the fundamental limits of privacy in public micro-data are not immune to breech. Under very mild assumptions about the distribution from which the records are drawn, an adversary with a small amount of background knowledge about an individual can use it to identify, with high probability, this individual's record in the anonymized dataset and to learn all anonymously released information about him or her, including sensitive attributes.[xvii]

While profiling may be a valuable tool in appropriate usages, and some of those usages may even be for security reasons, yet the very

means and methods used to fuel this process have direct implications to the erosion and subsequent loss of protection of one's personal privacy.

Some specific threats of profiling include:

1. Selection of advertising channels and messages based on each consumer's digital persona. To the extent that the digital persona is accurate, complete and up-to-date, this verges on consumer manipulation; and to the extent that it is not, it represents pre-judgment and denial of information;
2. Increased marketer power over consumers, through limitations on people's access to information about goods and services: the segmentation and marginalization of consumer information markets further limits the availability of information necessary for informed consumer choice, while simultaneously increasing consumer dependence upon the direct marketer's tightly managed information stream. The result is a market dominated by sellers. . . . The wider this information gap, the more difficult it becomes to ensure the equitable and efficient working of the marketplace; and
3. The combination of consumer profiling with ''geodemographic clustering'' techniques inevitably leads to ''electronic redlining.'' whereby calls from low-income neighborhoods (identified by their telephone exchange), can be routed to a busy signal, a long queue, or a recorded message suggesting that the desired information service is not presently available.[xviii]

The implications and risks of not only profiling but allowing the lines to be crossed between information collection for security purposes and information collection that erodes an individual's privacy, is evident in the following examples:

- Von's Supermarket of California sought to introduce ''loyalty card'' records in a court case where a consumer had slipped and injured himself in the store. Von's wished to prove that the customer may have been alcohol impaired, and that his loyalty card would show numerous purchases of alcohol. The evidence was ultimately never introduced.
- OnStar, rightfully so (after pressure from U.S. senators), decided to reverse its earlier decision to track the locations of its customers and potentially sell that information to third parties even after those customers have terminated their service plans with the company.
- Thomas Robins, a Virginia resident is suing Spokeo (www.spokeo.com) alleging that the company's collection and for-profit peddling of erroneous personal information has harmed his attempt to find a job. Robins claims that inaccurate information in his Spokeo profile ''caused actual harm'' to his employment prospects, according to his complaint,

A review of Spokeo's website privacy policy is an interesting example of the ramification to personal privacy when technology is not appropriately secured.

Spokeo aggregates publicly available information from phone books, social networks, marketing surveys, real estate listings, business websites, and other public sources (''Public Information''). This third-party data is then indexed through methods similar to those used by Google or Bing to create a listing. This Public Information may be made available to users through the Spokeo.com people search. Spokeo does

not verify and cannot guarantee the accuracy of this Public Information. Because Spokeo only collects this data and does not create it, we cannot fully guarantee its accuracy.[xix]

Has your organization considered these big data security (and tangentially related privacy) issues?

1. What if your data volume gets so large and varied you do not know how to deal with it?
2. How do you maintain the privacy of the data collected?
3. Do you analyze it all?
4. How can you find out which data points are really important?
5. Do you store all your data?
6. How can you use collected data to your best advantage?
7. How do you secure the data once collected?
8. What are the recovery options allocated to extreme volumes of collected data?

As the volume of personal identifiable data increases, as does its accuracy and the capabilities to collect, aggregate, disseminate, and use these data for commercial purposes, so will concerns about privacy and security. The union of these two worlds on the path to collision, is inevitable and both corporations and individuals need to be both cognizant and prepared for this inevitability.

"The United States faces the dual challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity, and free trade while also promoting safety, security, civil liberties, and privacy rights."
• President Barak Obama's Report on Cyber Security (May 30, 2009)

SOCIAL MEDIA, CORPORATE SECURITY, AND PERSONAL PRIVACY

IT security is no longer a technology issue. It is now a social issue, which deeply affects the lives of ordinary people.

When employees (and potentially contracted-employees) use their own personal mobile devices to transmit or store corporate information, this accentuates the risk that consumer IT poses to the confidentiality, integrity, availability, and security of enterprise resources along with the potential exposure to one's personal privacy.

Malicious apps can be developed to display pop-up boxes attempting to trick users into allowing access to their personal information and subsequently corporate data, which then could be transmitted back to attackers. As the rise in the use of location-aware apps and geo-marketing continue, concerns keep on growing around online privacy—specifically, business practices around the collection and use of the PII data.

Uses of the information are myriad, including direct marketing and context-sensitive content delivery, monitoring of criminals, enforcing location-based access restrictions on services, cloud balancing, and fraud detection and prevention. Geolocation technologies and their application, while offering social and economic benefit to a mobile society, raise significant privacy and risk concerns for individuals and businesses.[xx]

Employees also have a further expectation of privacy when they bring their own personal mobile devices to work. Employees rely on both the federal Computer Fraud and Abuse Act and its state counterparts.

"I particularly recognize that reasonable people can disagree as to what that proper balance or blend is between privacy and security and safety."
◆ *John Pistole*

- What if an employee with Company A creates a Twitter account, over time, amasses a large following, then leaves Company A for a competitor Company B, who owns the Twitter account? What if the employee created and updated the account on their own computing device and on their own time, away from the office?
- Do you let contractors hook their devices to your network?
- How do you manage data and privacy when employees are increasingly bringing their own mobile devices (BYOD) while meeting the needs of customers and partners that want to engage with your business anywhere, anytime?
- How do you enable trusted, high-quality interactions with management oversight at the network, device and application layer in order to manage the entire mobile ecosystem?
- Are company applications collecting PII? It may not always be obvious—for example, does your organization use persistent unique identifiers linked to central data stores containing personal information?
- Do organization-wide systems keep a record of consent to the transfer of PII? This record should be available to the user (consider also the value of keeping server-side records attached to any user data stored). Such records themselves should minimize the amount of personal data they store (e.g., using hashing).
- Is an assessment conducted to determine whether your consent collection mechanism overlaps or conflicts (e.g., with the data handling practices stated in company policies) with any other consent collection practices?

To address protection of employee privacy has your organization:

- Established a mobile policy based on employee-owned devices or a hybrid of employee and corporate-owned devices?
- Implemented mobile security and device management solution that maintains employee privacy?
- Identified employee responsibility for managing the provider, data plan, and costs incurred?
- Isolated and secured corporate data from personal data on devices?
- Set privacy policies that do not collect personal data?
- Customized policies based on device ownership?
- Defined granular policies to prevent collection of Global Positioning System (GPS), user info, app lists, and telecom data?

To address legal obligations, mitigate risks, and maintain the flexibility to stay out in front of a changing data privacy and security landscape, organizations should develop comprehensive data privacy and security infrastructures.

Principal components of a comprehensive privacy program should include:

- Accountability
- Risk assessment
- Privacy and security safeguards
- Service provider management
- Incident response procedures
- Continual evaluation and improvement

WORKING 9 TO 5: PRIVACY IN THE WORKPLACE

From e-mail monitoring and website blocking to phone tapping and GPS tracking, employers increasingly combine technology with policy to manage productivity and minimize litigation, security, and other risks.

Concern over litigation and the role electronic evidence plays in lawsuits and regulatory investigations has spurred more employers to monitor online activity. Data security and employee productivity concerns also motivate employers to monitor Web and e-mail use and content.

According to the most recent study, the "2007 Electronic Monitoring & Surveillance Survey" from American Management Association (AMA) and The ePolicy Institute, computer monitoring takes many forms:

- 45% of employers tracking content, keystrokes, and time spent at the keyboard
- 43% store and review computer files
- 12% monitor the blogosphere to see what is being written about the company
- 10% monitor social networking sites

Of the 43% of companies that monitor e-mail, 73% use technology tools to automatically monitor e-mail and 40% assign an individual to manually read and review e-mail.[xxi]

While employees have a legitimate expectation of privacy in the workplace, this right must be balanced with the rights and interests of the employer. In particular, the employer's right to run their business efficiently and above all, to protect themselves from any liability or harm an employee's actions may create.

These rights and interests constitute legitimate grounds that may justify appropriate measures to limit the worker's right to privacy. Examples of these could include:

- Where the employer is victim of a worker's criminal offense
- Where the employees' use of social networking sites causes damage to the employer's business reputation or releases confidential information
- Dealing with cyberbullying in the workplace, that is, bullying carried out on the Internet and mobile phones, through social networking sites, e-mail, and texts. You can read more about bullying in the workplace.[xxii]

However, balancing different rights and interests requires taking a number of principles into account, in particular, proportionality. It should be clear that the simple fact that a monitoring activity or surveillance is considered convenient to serve the employer's interest would not solely justify any intrusion into a worker's privacy.

What personal information is available to employers? Once you give your consent, employers have broad latitude to inquire into your background. A quick review of information available to employers, if when collected is used improperly or not properly secured, would significantly impact an employee's privacy, include but is not limited to:

- Character reference check
- Identity and address verification
- Identity History Summary (money laundering check)
- Identity and terrorist check
- Credit history validation
- Tax information
- Criminal Records
- Civil Judgments
- Bankruptcies
- Professional Licenses
- Tax Liens
- Verification of validity of passports for citizenship, immigration, or legal work status
- Criminal, arrest, incarceration, and sex offender records
- Military records
- Driving and vehicle records
- Education records
- Employment records
- Medical, Mental, and Physiological evaluation and records
- Drug tests and polygraph testing results
- Social Security Number

Balancing the legitimate need of employers to monitor the workplace with respect for individual privacy is not difficult. The best course of action is to have a monitoring policy and follow it. Legal experts state that apathy toward e-mail and Internet policies is the biggest mistake an employer can make.

It is recommended that firms have a written policy clearly stating that any right to privacy is waived for documents and messages created, stored, sent or received on the firm's computer systems or over its networks.

Achieving balance may require a reasonable monitoring policy that also sets individual privacy expectations (see Table 3). Legal analysts advise that setting policies with clearly stated monitoring intentions is the most important action employers can take to minimize invasion of privacy claims.

Clear-cut policies set boundaries, establish employees' expectations of privacy, and help set a workplace tone that conveys organizational responsibility and respect for others.

At the minimum, comprehensive monitoring policies should:

- State the specific business purposes for monitoring
- Clearly state the ownership of company computers, networks, files, and e-mail

Table 3 ***Organizations Assisting Employees with Workplace Privacy Issues***

9 to 5, the National Association of Working Women	www.9to5.org
American Civil Liberties Union	www.aclu.org
National Work Rights Institute	www.workrights.org
Workplace Fairness	www.workplacefairness.org

- Clearly outline the forms of communication considered illegal, prohibited, and unacceptable
- Clearly outline the websites considered illegal, prohibited, and unacceptable
- Define the acceptable use of company networks and e-mail
- Set clear boundaries for the personal use of company networks
- Inform employees of the specific types of monitoring activities that will be used
- Explain how monitoring activities are advantageous to employees, clients, and the company
- Determine the consequences for policy violations.[xxiii]

"The government must give proper weight to both keeping America safe from terrorists and protecting Americans' privacy. But when Americans lack the most basic information about our domestic surveillance programs, they have no way of knowing whether we're getting that balance right. This lack of transparency is a big problem."
◆ *Al Franken*

"I think we're seeing privacy diminish, not by laws . . . but by young people who don't seem to value their privacy."
◆ *Alan Dershowitz*

SUMMARY

Achieving the balance between privacy and security was never an easy task; doing so in today's digitally connected, 24/7 access to information, "always on," global society, is daunting—some may argue, even impossible.

Corporate security has become a high-profile issue since the events of September 11, 2001, gone are the days of single fire walls, periodic malware updates, and annual security audits. Advancing technology has changed IT and related security forever, security must be a 24/7 philosophy.

In order to protect corporate data, we must secure devices and documents with passwords and store data in approved locations. While following corporate security guidelines is often an inconvenience, the necessity is clear. Much of the data we create and store on corporate networks contains trade secrets, personally identifiable information, or potentially privileged communications and we have an obligation to protect those data on behalf of corporate interests.[xxiv]

The responsibility to protect one's privacy to keep private information private falls ultimately to the individual. While technology pushes forward with both the ways and means to wrest that privacy from us, we are still the strongest, first line of defense.

Due diligence with respect to protecting your private information is paramount, thinking prior to communicating personal information pivotal, refusing to provide personal information (within the boundaries of legally acceptable practice) without first knowing, verifying, and feeling comfortable as to its usage, takes practice, fortitude, and perseverance.

Proactive management of both necessary security measures developed, implemented, and managed in concert with equally necessary privacy practices, will be essential for sustaining our global society through the coming decades of the 21st century and beyond.

Notes

i. Deere, S. (April 16, 2014). "Six Flags Season Pass Holders Now Must Provide a Finger Scan," The St. Louis Post-Dispatch, www.stltoday.com/news/local/metro/six-

flags-season-pass-holders-now-must-provide-a-finger/article_713d3869-8eae-594e-8399-5117f088bef5.html (retrieved April 2014).

ii. EPIC v. DOJ—Pen Register Reports, http://epic.org/foia/doj/pen-reg-trap-trace/#SAR (retrieved April 2014).

iii. Semiannual Report of the Attorney General on Electronic Surveillance and Physical Search under the Foreign Intelligence Surveillance Act, http://epic.org/foia/doj/pen-reg-trap-trace/025.%20June%202013%20SAR%20%5BPRTT%20pages%5D-OCR.pdf (retrieved April 2014).

iv. The provisions of Executive Order 12333 of December 4, 1981, appear at 46 FR 59941, 3 CFR, 1981 Comp., p. 200.

v. Moteff, J. (April 16, 2004). "Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives, Congressional Research Service," The Library of Congress, www.fas.org/irp/crs/RL32357.pdf (retrieved April 2014).

vi. Horowitz, R. "Summary of Key Sections of the USA Patriot Act of 2001," www.rhesq.com/Terrorism/Patriot_Act_Summary.pdf (retrieved April 2014).

vii. Nice, K. "How Car Computers Work," http://auto.howstuffworks.com/under-the-hood/trends-innovations/car-computer.htm (retrieved April 2014).

viii. Office of the Federal Register. 2006. National Highway Traffic Safety Administration—Final Rule. Docket no. NHTSA–2006–25666; 49 CFR Part 563 Event data recorders. Federal Register, vol. 71, no. 166, pp. 50998–51048. Washington, DC: National Archives and Records Administration.

ix. National Highway Traffic Safety Administration Event Data Recorder Working Group. 2001. Event data recorders: summary of findings. Final report. Washington, DC: U.S. Department of Transportation, and Gabler, H. C., Gabauer, D. J., Newell, H. L, and O'Neill, M.E. 2004. Use of Event Data Recorder (EDR) Technology for Highway Crash Data Analysis. NCHRP Project no. 17–24; Contractor's final report. Washington, DC: Transportation Research Board.

x. Mitchell, R. (April 21, 2014). "4 Things to Do Now To Get Ready For the Internet of Things," www.computerworld.com/s/article/9247616/4_things_to_do_now_to_get_ready_for_the_Internet_of_Things? taxonomyId=16 (retrieved April 2014).

xi. Internet of Things (IoT). WhatIs.com, http://whatis.techtarget.com/definition/Internet-of-Things (retrieved April 2014).

xii. Process Automation Control, www.pacontrol.com/wireless-standards.html (retrieved April 2014).

xiii. Osborne, C. (June 12, 2012). "Are Smart Meters a Privacy Risk?" www.smartplanet.com/blog/smart-takes/are-smart-meters-a-privacy-risk (retrieved April 2014).

xiv. Narayanan, A., and Shmatikov, V. "Robust De-Anonymization of Large Sparse Datasets," in 2008 IEEE Symposium on Security and Privacy (sp 2008). IEEE, May

2008, pp. 111–125, www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (retrieved April 2014).

xv. Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., and Byers, A. H. "Big Data: The Next Frontier for Innovation, Competition, and Productivity," The McKinsey Global Institute, Tech. Rep., May 2011, www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_ for_innovation (retrieved April 2014).

xvi. Hasan, O., Habegger, B., Brunie, L., Bennani, N., and Damiani, E. "A Discussion of Privacy Challenges in User Profiling with Big Data Techniques: The EEXCESS Use Case," http://eexcess.eu/wp-content/uploads/2013/07/2013.07_ BigData-2013-04.pdf (retrieved April 2014).

xvii. Narayanan, A., and Shmatikov, V. "Robust De-Anonymization of Large Sparse Datasets," in 2008 IEEE Symposium on Security and Privacy (sp 2008). IEEE, May 2008, pp. 111–125, www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (retrieved April 2014).

xviii. Clarke, R. "Customer Profiling and Privacy Implications for the Finance Industry," www.rogerclarke.com/DV/CustProfFin.html (retrieved April 2014).

xix. Privacy Policy, Spokeo, www.spokeo.com/privacy/terms (retrieved May 2014).

xx. "Geolocation Risk, Issues and Strategies" (September 2011). An ISACA Emerging Technology White Paper, www. isaca.org/Knowledge-Center/Research/ResearchDeliverables/ Pages/Geolocation-Risks-Issues-and-Strategies.aspx (retrieved May 2014).

xxi. The Latest on Workplace Monitoring and Surveillance, American Management Association and The ePolicy Institute. Last updated August 5, 2010, www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx (retrieved may 2014).

xxii. "Surveillance in the Workplace," Citizens Information Board, www.citizensinformation.ie/en/employment/employment_rights_and_conditions/monitoring_and_surveillance_at_work/surveillance_of_electronic_communications_in_the_workplace.html (retrieved May 2014).

xxiii. Wakefield, R. "Employee Monitoring and Surveillance—The Growing Trend," *Information Systems Control Journal*, *1* (2004), www.isaca.org/Journal/Past-Issues/2004/Volume-1/Pages/Employee-Monitoring-and-Surveillance-The-Growing-Trend.aspx (retrieved May 2014).

xxiv. Carns, D. (February 7, 2014). "Four Broad Considerations in Modern Data Security and What You Can Do to Make Necessary Changes," www.insidecounsel.com/2014/02/07/technology-securing-corporate-data-in-an-internet (retrieved May 2014).

Albert J. Marcella Jr., Ph.D., CISA, CISM, is president of Business Automation Consultants, LLC. Dr. Marcella, is an internationally recognized public speaker, researcher, and workshop and seminar leader with over 35 years of experience

in IT audit, security, and assessing internal controls. Dr. Marcella, has authored numerous articles and 29 books on various IT, audit, and security related subjects.

Carol Stucki, CISA, PMP, is a Project Manager with over 25 years of experience in operational and IT roles including providing internal systems consulting, portfolio management, and auditing services for companies both in the Unites States and abroad. Carol has worked for GTE (now Verizon), Arthur Andersen, Perot Systems, Los Alamos National Labs on DOE, DOD, HSD contracts, Church of Jesus Christ of Latter-day Saints, Capgemini, and HealthNow.