Preface

Let’s Call it the “Security and Privacy Decade”: The Consequence of Pervasive Information Technology

ABSTRACT

Pervasiveness of information technology (IT) in our lives is well underway when considering IT permeates and impacts all aspects of everything we do to the extent that we would notice its absence more intensely than we would its presence. Advances in computing and communication networks have contributed to this expanding role by making IT cheaper, faster, and more powerful resulting in capabilities that allow us to utilize information technology in ways previously unimaginable. Although this technological revolution has brought us closer and has made our lives easier and more productive, paradoxically, it has also made us more capable of harming one another and more vulnerable to be harmed by each other. Our vulnerabilities are the consequence of our capabilities. What are the security and privacy implication of this expanding role of IT? In this chapter, we discuss how the role of information technology is changing and how this change impacts information security and privacy. The evolving nature of information security and privacy brings additional challenges and opportunities that we, as a society, need to understand and prepare for in order to take full advantage of advances in information technology.

INTRODUCTION

The role of Information Technology (IT) in our lives is expanding. Pervasiveness of information technology (IT) in our lives is well underway when considering IT permeates and impacts all aspects of everything we do to the extent that we would notice its absence more intensely then we would its presence. Advances in computing and communication networks have contributed to this expanding role by making IT cheaper, faster, and more powerful resulting in capabilities that allow us to utilize information technology in ways previously unimaginable. We are the first generation of humans where the capabilities of the technologies that support our information processing activities are truly revolutionary and far exceed those of our forefathers. We speak of the age we line in as the “information age” and our society
as “information society”. The emergence of the society based on information signals a transition toward a new society based on the production and exchange of information as opposed to physical goods (Stephanidis et al., 1984). Information Society refers to the new socioeconomic and technological paradigms that affect human activities, individual behaviors, our collective consciousness, and our economic and social environments. The information age has important consequences for our lives as well. Essentially, it has ushered a new range of emerging computer-mediated activities that have revolutionized the way we live and interact with one another (Mesthene 1968; Nardi, 1996; Stephanidis et al., 1984). More people are employed generating, collecting, handling, processing and distributing information than any other profession and in any other time (Mason 1986). IT has made us more productive in our workplaces, has brought us closer, transformed our lives and has helped in redefining who we are as humans. We are able to communicate more freely and effortlessly with one another, make more informed decisions, and have a higher standard of living, all, resulting from advances in Information Technologies (IT). Its impacts can be felt in the ways in which we relate, interact, and communicate not just with one another but also the way we interact with the technology itself. To some extent, information technologies have become “information appliances”. IT has also redefined our relationships with businesses we interact with and governmental agencies representing us. As a result, our world has been altered so irrevocably that we are no longer able to conduct our lives without it. Yet, many experts believe that we have only seen the tip of the iceberg. We are on the verge of the biggest societal transformation in the history of mankind traced directly to advances in the information technology. This transformation will most likely create new opportunities and challenges we have yet to fathom. But the greatest impact of all will be in the way we perceive and identify ourselves as individuals.

Information defines us. It defines the age we live in and the societies we inhibit. Information is the output of our human intellectual endeavors which inherently defines who we are as humans and how we conduct our lives. New technologies make possible what was not possible before. This alters our old value clusters whose hierarchies were determined by range of possibilities open to us at the time. By making available new options, new technologies can and will lead to a restructuring of the hierarchy of values (Mesthene, 1968). Mason argues that unique challenges facing our information society are the result of the evolving nature of information itself. Mason argues that in this age of information, a new form of social contract is needed in order to deal with the potential threats to the information which defines us. Although this technological revolution has brought us closer and has made our lives easier and more productive, paradoxically, it has also made us more capable of harming one another and more vulnerable to be harmed by each other. Our vulnerabilities are the consequence of our capabilities. Mason (1986) states “Our moral imperative is clear. We must insure that information technology, and the information it handles, are used to enhance the dignity of mankind. To achieve these goals we much formulate a new social contract, one that insures everyone the right to fulfill his or her own human potential.” (Mason, 1986, p 26). In light of the Aristotelian notion of the intellect, this new social contract has a profound implication in the way our society views information and the technologies that support them. For IT to enhance the “human dignity”, it should assist humans in exercising their intellects ethically. But is it possible to achieve this without assuring the trustworthiness of information and the integrity of the technologies we are using? Without security that guarantees the trustworthiness of information and the integrity of our technologies, appropriate uses of that information cannot be realized. This implies that securing information and privacy of that information are inherently intertwined and should be viewed...
synergistically. As a result, Information security and privacy have been viewed as the foremost areas of concern and interest by academic researchers and industry practitioners from a wide spectrum of different disciplines alike. We define Information security and privacy as an all encompassing term that refers to all activities needed to assure privacy of information and security of systems that support it in order to facilitate its use.

We have entered an exciting period of unparalleled interest and growth in research and practice of all aspects of information security and privacy. Information security and privacy is the top IT priority facing organizations. According to the 20th Annual Top Technology Initiatives survey produced by the American Institute of Certified Public Accountants (AICPA, 2009) information security tops the list of ten most important IT priorities (http://infotech.aicpa.org/Resources/). According to the survey results, for the seventh consecutive year, Information Security is identified as the technology initiative expected to have the greatest impact in the upcoming year for organizations and is thus ranked as the top IT priority for organizations. This is first year that information privacy has shot up to second most important IT priority. This is very significant that top two issues are information security and privacy and the six out of the top ten technology initiatives discussed in this report are issues related to information security and privacy (AICPA 2009). The interest in all aspects of information security and privacy is also manifested by the recent plethora of books, journal articles, special issues, and conferences in this area. This has resulted in a number of significant advances in technologies, methodologies, theories and practices of information security and privacy. These advances, in turn, have fundamentally altered the landscape of research in a wide variety of disciplines, ranging from information systems, computer science and engineering to social and behavioral sciences and the law. This confirms what information security and privacy professionals and researchers have known for a long time that information security and privacy is not just a “technology” issue any more. It impacts and permeates almost all aspects of business and the economy.

Until recently, information security and privacy were exclusively discussed in terms of mitigating risks associated with data and the organizational and technical infrastructure that supported it. With the emergence of the new paradigm in information technology, the role of information security and ethics has evolved. As Information Technology and the Internet become more and more ubiquitous and pervasive in our daily lives, a more thorough understanding of issues and concerns over the information security and ethics is becoming one of the hottest trends in the whirlwind of research and practice of information technology. This is chiefly due to the recognition that whilst advances in information technology have made it possible for generation, collection, storage, processing and transmission of data at a staggering rate from various sources by government, organizations and other groups for a variety of purposes, concerns over security of what is collected and the potential harm from personal privacy violations resulting from their unethical uses have also skyrocketed. Therefore, understanding of pertinent issues in information security and privacy vis-à-vis technical, theoretical, managerial and regulatory aspects of generation, collection, storage, processing, transmission and ultimately use of information are becoming increasingly important to researchers and industry practitioners alike. Information security and privacy have been viewed as one of the foremost areas of concern and interest by academic researchers and industry practitioners from diverse fields such as engineering, computer science, information systems, and management. Recent studies of major areas of interest for IT researchers and professionals point to information security and privacy as one of the most pertinent.
Data, Data, Data Everywhere

A byproduct of pervasiveness of Information Technology is the amazingly large amount of data currently being generated. This data needs to be stored securely and privately. According to IBM (IBM 2010), worldwide data volumes are currently doubling every two years. Data experts estimate that in 2002 the world generated 5 exabytes of data. This amount of data is more than all the words ever spoken by human beings. The rate of growth is just as staggering – the amount of data produced in 2002 was up 68% from just two years earlier. The size of the typical business database has grown a hundred-fold during the past five years as a result of internet commerce, ever-expanding computer systems and mandated recordkeeping by government regulations. The rate of growth in data has not slowed. International Data Corporation (IDC) estimates that the amount of data generated in 2009 was 1.2 million Petabytes (IDC, 2010). (A Petabyte is a million gigabytes.) (IDC Report, 2010). Although this seems to be an astonishingly large amount of data, it is paled in compression to what IDC estimates that amount to be in 2020. IDC estimates that the amount of data generated in 2010 will 44 times as much as this year to an incomprehensible amount of 35 Zettabytes (A Zettabyte is 1 trillion gigabytes). IDC reports that by 2020, we will generate 35 trillion gigabytes of data. To better grasp how much data this is, consider the following: if one byte of data is the equivalent of this dot (•), the amount of data produced globally in 2009 would equal the diameter of 10,000 suns.

One of the reasons for this astonishingly large growth, according to a survey by US Department of Commerce, is that an increasing number of Americans are going online and engaging in several online activities, including online purchases, conducting banking online, engaging in commerce, and interacting socially. The growth in Internet usage and e-commerce has offered businesses and governmental agencies the opportunity to collect and analyze information in ways never previously imagined. “Enormous amounts of consumer data have long been available through offline sources such as credit card transactions, phone orders, warranty cards, applications and a host of other traditional methods. What the digital revolution has done is increase the efficiency and effectiveness with which such information can be collected and put to use” (Adkinson, Eisenach, & Lenard, 2002).

Almost everything that we do in our daily lives can generate a digital footprint. Whether we are using credit cards, surfing the Internet or viewing a YouTube video, we are generating data. IDC senior vice president, John Gantz states: “About half of your digital footprint is related to your individual actions—taking pictures, sending e-mails, or making digital voice calls. The other half is what we call the ‘digital shadow’—information about you—names in financial records, names on mailing lists, web surfing histories or images taken of you by security cameras in airports or urban centers. For the first time your digital shadow is larger than the digital information you actively create about yourself.” Our digital shadow, the sum of all the digital information generated about us on a daily basis, now exceeds the amount of digital information we actively create ourselves (IDC, 2010). This digital footprint including our digital shadow represents us, as humans, it represents who we are, and how we conduct our lives. It needs to be secured, protected, and managed appropriately.

This proclamation about data volume growth is no longer surprising, but continues to amaze even the experts. For businesses, more data isn’t always better. Organizations must assess what data they need to collect and how to best leverage it. Collecting, storing and managing business data and associated databases can be costly, and expending scarce resources to acquire and manage extraneous data fuels inefficiency and hinders optimal performance. The generation and management of business data also loses much of its potential organizational value unless important conclusions can be extracted from it
quickly enough to influence decision making while the business opportunity is still present. Managers must rapidly and thoroughly understand the factors driving their business in order to sustain a competitive advantage. Organizational speed and agility supported by fact-based decision making are critical to ensure an organization remains at least one step ahead of its competitors. Several studies (Brancheau, Janz, & Wetherbe, 1996; Niederman, Brancheau, & Wetherbe, 1991) have shown that data has been ranked as one of the top priorities for IT executives as an organizational resource. Similar research (Rockart & DeLong, 1988; Watson, Rainer Jr, & Koh, 1991) has also revealed that data is an important part of a decision support system since it forms the basis of the information that is delivered to decision makers. The formidable challenge facing organizations involves the collection, management, and presentation of its data to enable management to make well-informed and timely decisions. With the emergence of web technologies, the collection and storage of data, both internal and external to an organization, has increased dramatically. In spite of this enormous growth in enterprise databases, research from IBM reveals that organizations use less than 1 percent of their data for analysis (Brown, 2002). This is the fundamental irony of the information age we live in: Organizations possess enormous amounts of business data, yet have so little real business information, and to magnify the problem further, a leading business intelligence firm recently surveyed executives at 450 companies and discovered that 90 percent of these organizations rely on instinct rather than hard facts for most of their decisions because they lack the necessary information when they need it (Brown, 2002). Moreover, in cases where sufficient business information is available, organizations are only able to utilize less than 7 percent of it (Economist, 2001).

**Information Security**

Information is a critical asset that supports the mission of an organization. Protecting this asset is critical to survivability and longevity of any organization. Maintaining and improving information security is critical to the operations, reputation, and ultimately the success and longevity of any organization. However, Information and the systems that support it are vulnerable to many threats that can inflict serious damage to organizations resulting in significant losses. The concerns over information security risks can originate from a number of different security threats. They can come from hacking and unauthorized attempts to access private information, fraud, sabotage, theft and other malicious acts or they can originate from more innocuous sources, but no less harmful, such as natural disasters or even user errors. David Mackey, IBM’s Director of security intelligence estimates that IBM recorded more than 1 billion suspicious computer security events in 2005. He estimates that a higher level of malicious traffic in 2006. The damage from these “security events” can range from lose of integrity of the information to total physical destruction or corruption of entire infrastructure that support it. The damages can stem from the actions of a variety of sources, such as disgruntle employees defrauding a system or careless errors committed by trusted employees to hackers gaining access to the system from outside of the organization. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are “swept under the carpet” to avoid unfavorable publicity. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system. Broadly speaking the main purpose of information security is to protect an organization’s valuable resources, such as information, hardware, and software.

The importance of securing our information infrastructure is not lost to the government of the United States. The US Department of Homeland Security (DHS) identifies a Critical Infrastructure (CI) as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or
destruction of such systems and assets would have a debilitating impact on security, national economic
security, national public health or safety, or any combination of those matters.” According a recent report
by the DHS titled The National Strategy for Homeland Security, which identified thirteen CI’s, disrup-
tion in any components of a CI can have catastrophic economic, social and national security impacts.
Information Security is identified as a major area of concern for the majority of the thirteen identified
CI’s. For example, many government and private-sector databases contain sensitive information which
include personally identifiable data such as medical records, financial information such as credit
card numbers, and other sensitive proprietary business information or classified security-related data.
Securing these databases which form the back bone of a number of CI’s is of paramount importance.
Losses due to electronic theft of information and other forms of cybercrime against to such databases
can result in tens of millions of dollars annually.

Information security is concerned with the identification of electronic information assets and the
development and implementation of tools, techniques, policies, standards, procedures and guidelines to
ensure the confidentiality, integrity and availability of these assets. Although Information Security can
be defined in a number of ways, the most salient is set forth by the government of the United States. The
National Institute of Standards and Technology (NIST) defines Information Security based on the 44
United States Code Section 3542(b)(2), which states “Information Security is protecting information and
information systems from unauthorized access, use, disclosure, disruption, modification, or destruction
in order to provide integrity, confidentiality, and availability.” (NIST, 2003, p3). The Federal Informa-
tion Security Management Act (FISMA, P.L. 107-296, Title X, 44 U.S.C. 3532) defines Information
Security as “protecting information and information systems from unauthorized access, use, disclosure,
disruption, modification, or destruction” and goes on to further define Information Security activities as
those “carried out in order to identify and address the vulnerabilities of computer system, or computer
network” (17 U.S.C. 1201(e), 1202(d)). The United States’ National Information Assurance Training
and Education Center (NIATEC) defines information security as “a system of administrative policies
and procedures” for identifying, controlling and protecting information against unauthorized access to
or modification, whether in storage, processing or transit” (NIATEC, 2006).

The overall goal of information security should be to enable an organization to meet all of its mis-
sion critical business objectives by implementing systems, policies and procedures to mitigate IT-related
risks to the organization, its partners and customers (NIST, 2004). The Federal Information Processing
Standards Publication 199 issued by the National Institute of Standards and Technology (NIST, 2004)
defines three broad information security objectives: Confidentiality, Integrity and Availability. This trio
of objectives sometimes is referred to as the “CIA Triad”.

- **Confidentiality:** “Preserving authorized restrictions on information access and disclosure, includ-
ing means for protecting personal privacy and proprietary information…” [44 U.S.C., Sec. 3542].
  Confidentiality is the assurance that information is not disclosed to unauthorized individuals,
  processes, or devices (NIST, 2003 p. 15). Confidentiality protection applies to data in storage,
  during processing, and while in transit. Confidentiality is extremely important consideration for
  any organization dealing with information and is usually discussed in terms of privacy. A loss of
  confidentiality is the unauthorized disclosure of information.
- **Integrity:** To ensure that timely and reliable access to and use of information is possible. According
to 44 United States Code Section 3542(b)(2), integrity is defined as “guarding against improper
information modification or destruction, and includes ensuring information non-repudiation and
authenticity…” Therefore, integrity is interpreted to mean protection against is the unauthorized
modification or destruction of information. Integrity should be viewed both from a “data” and a
“system” perspective. Data integrity implies that data has not been altered in an unauthorized man-
ner while in storage, during processing, or while in transit. System integrity requires that a system
is performing as intended and is not impaired and is free from unauthorized manipulation (NIST,
2003).

• **Availability:** Timely, reliable access to data and information services for authorized users (NIST,
2003). According to 44 United States Code Section 3542(b)(2), availability is “Ensuring timely and
reliable access to and use of information…”. Availability is frequently viewed as an organization’s
foremost information security objective. Information availability is a requirement that is intended
to assure that all systems work promptly and service is not denied to authorized users. This should
protect against the intentional or accidental attempts to either perform unauthorized access and
alteration to organizational information or otherwise cause a denial of service or attempts to use
system or data for unauthorized purposes. A loss of availability is the disruption of access to or use
of information or an information system.

In defining the objectives of information security, there are a number of extensions to the CIA Triad.
Most prominent extensions to the CIA Triad include three additional goals of Information Security. They
are: accountability, authentication, and norrepudiation. One such extension appears in the National Secu-
ritiy Agency (NSA) definition of information security as “… measures that protect and defend information
and information systems by ensuring their availability, integrity, authentication, confidentiality, and
nonrepudiation. These measures include providing for restoration of information systems by incorporat-
ing protection, detection, and reaction capabilities.”(CNSS, 2003) This definition is almost identical to
the way “cybersecurity” was defined by the 108th US Congress. A cybersecurity bill introduced in the
Thornberry; reintroduced in the 109th Congress as H.R. 285 where cybersecurity is defined as …the
prevention of damage to, the protection of, and the restoration of computers, electronic communications
systems, electronic communication services, wire communication, and electronic communication, in-
cluding information contained therein, to ensure its availability, integrity, authentication, confidentiality,
and nonrepudiation.

• **Accountability:** Is the cornerstone of organizational information security objective in which auditing
capabilities are established to ensure that users and producers of information are accountable for
their actions and to verify that organizational security policies and due diligence are established,
enforced and care is taken to comply with any government guidelines or standards. Accountability
serves as a deterrent to improper actions and as an investigation tool for regulatory and law
enforcement agencies.

• **Authentication:** Security measure designed to establish the validity of a transmission, message,
or originator, or a means of verifying an individual’s authorization to receive specific categories
of information (CNSS, 2003. p 5). In order for a system to achieve security, it should require that
all users identify themselves before they can perform any other system actions. Once the identifi-
cation is achieved the authorization should be the next step. Authorization is process of granting
permission to a subject to access a particular object. Authentication is the process of establishing
the validity of the user attempting to gain access, and is thus a basic component of access control,
in which unauthorized access to the resources, programs, processes, systems are controlled. Access control can be achieved by using a combination of methods for authenticating the user. The primary methods of user authentication are: access passwords, access tokens, something the user owns which can be based on a combination of software or hardware that allows authorized access to that system (e.g., smart cards and smart card readers), the use of biometrics (something the user is, such as a fingerprint, palm print or voice print), access location (such as a particular workstation), user profiling (such as expected or acceptable behavior), and data authentication, to verify that the integrity of data has not been compromised. (CNSS, 2003)

**Nonrepudiation:** Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the data. (CNSS, 2003)

Any information security initiative aims to minimize risk by reducing or eliminating threats to vulnerable organizational information assets. The National Institute of Standards and Technology (NIST, 2003, p. 7) defines risk as “…a combination of: (1) the likelihood that a particular vulnerability in an agency information system will be either intentionally or unintentionally exploited by a particular threat resulting in a loss of confidentiality, integrity, or availability, and (2) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability will have on agency operations (including mission, functions, and public confidence in the agency), an agency’s assets, or individuals (including privacy) should there be a threat exploitation of information system vulnerabilities.” Risks are often characterized qualitatively as high, medium, or low. (NIST, 2003, p 8). The same publication defines threat as “…any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability,” and vulnerability as “…a flaw or weakness in the design or implementation of an information system (including security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect an agency’s operations (including missions, functions, and public confidence in the agency), an agency’s assets, or individuals (including privacy) through a loss of confidentiality, integrity, or availability” (NIST, 2003, 9). NetIQ (2004) discusses five different types of vulnerabilities that have direct impact on the governance of information security practices. They are: exposed user accounts or defaults, dangerous user behavior, configuration flaws, missing patches and dangerous or unnecessary service. An effective management of these vulnerabilities is critical for three basic reasons. First, an effective vulnerability management helps reducing the severity and growth of incidence. Second, it helps in regulatory compliance. And third and the most important reason can be summed as simply saying, it is a “good business practice” to be proactive in managing the vulnerabilities rather than be reactive by trying to control the damage from an incidence.

**Information Privacy**

Privacy is defined as “the state of being free from unsanctioned intrusion” (Dictionary.com, 2006). Westin (Westin, 1967) defined the right to privacy as “the right of the individuals… to determine for themselves when, how, and to what extent information about them is communicated to others.” The Fourth Amendment to the US Constitution’s Bill of Rights states that “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” This belief carries back through history in such expressions from England, at least circa 1603, “Every
man’s house is his castle.” The Supreme Court has since ruled that “We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts.” Thus, because the Amendment “protects people, not places,” the requirement of actual physical trespass is dispensed with and electronic surveillance was made subject to the Amendment’s requirements (Findlaw.com, 2006). Generally the definitions of privacy in regards to business are quite clear. On the Internet, however, privacy raises greater concerns as consumers realize how much information can be collected without their knowledge. Companies are facing an increasingly competitive business environment which forces them to collect vast amounts of customer data in order to customize their offerings. Eventually, as consumers become aware of these technologies new privacy concerns will arise, and these concerns will gain a higher level of importance. The security of personal data and subsequent misuse or wrongful use without prior permission of an individual raise privacy concerns and often end up in questioning the intent behind collecting private information in the first place (Dhillon & Moores, 2001). Privacy information holds the key to power over the individual. When privacy information is held by organizations that have collected the information without the knowledge or permission of the individual the rights of the individual are at risk. Individual data privacy has become a prominent issue in the United States (Dyson, 1998). In a revealing interview with MSNBC, Eric Schmidt, CEO of Google, repeated a frequently heard mantra “that if you do not want people to know what you are doing on-line, maybe you shouldn’t be doing it” (Rapoza, 2010). The view of privacy concerns promoted widely is misguided at best and completely disingenuous at worst. However, for most of us, this is the prevailing view of privacy suggesting a fundamental misunderstanding of what it is all about. In his article “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy,” Daniel Solove provides a strong rebuttal to this line of reasoning and points out the fundamental fallacies associated with it. He argues this notion stems from a fallacious conceptualization of privacy and concedes that privacy is an “exasperatingly vague and evanescent” concept to define (Miller, 1971). It is a concept so “infected with pernicious ambiguities” (Gross, 1967) and “so complex, so entangled in competing and contradictory dimensions, so enmeshed with various and distinct meanings,” that it may never be fully understood (Post, 2001). In defining privacy, Solove states that “[privacy] is not the trumpeting of the individual against society’s interests, but the protection of the individual based on society’s own norms and values. Privacy is not simply a way to extricate individuals from social control, as it is itself a form of social control that emerges from society’s norms. It is not an external restraint on society, but is in fact an internal dimension of society. Therefore, privacy has a social value. Even when it protects the individual, it does so for the sake of society. It thus should not be weighed as an individual right against the greater social good. Privacy issues involve balancing societal interests on both sides of the scale.” (Solove, 2007, page 763)

I recently taught a graduate course in data privacy. One of the course assignments required students to analyze privacy policies of number of most popular web sites. Most students were astonished by how complex these policies were and how hard they were to understand. For example, the privacy policy of Facebook is now longer than the US Constitution with almost 50 settings and more than 170 options available to the users. Given such a large number of options and settings, how likely is for an average user to understand and to make an informed decision about which privacy settings are most appropriate to their needs. The complexities of these privacy policies make it very difficult, if not impossible, for ordinary users to comprehend the consequences of their privacy choices. Consider this; in a response to privacy critiques and in an attempt to make the Facebook the “social center of the web”, in April 2010, Facebook announced new privacy policies which included the development of “Open Graphs”, as a
platform for developers to exchange ideas and information. Open Graphs is an extension of the idea of “semantic networks”, which according to Tim Berners-Lee (1999), is an attempt to “bring structure to the meaningful content of Web pages thus enabling computers to understand that content and how it relates to other sites and information across the internet”. Open Graphs gives Facebook the ability to integrate websites and web apps within its existing social network environment by allowing its partner sites to create categories based on users’ interests and then exchange that information with one another. For example, Open Graph would make the following scenario possible. A Facebook user visits Netflex, a movie rental site, and searches for a movie to rent. Netflex, an Open Graph partner of Facebook, develops a customized review for this user based on the reviews of that movie and similar other movies uploaded by the user’s Facebook friends. Once the user makes the final selection, Netflex in turn, can notify the user’s Facebook friends that their movie reviews were used by the user and thereby revealing what movie the user rented. Although this is an innocuous example of what is possible, more nefarious scenarios can be envisioned. The privacy consequence of Open Graphs is far reaching and not yet well understood, not even by the experts, let alone the average user. The most significant privacy consequence of Open Graphs is the redefinition of what “public” means. Users need to understand that public no longer means public within the Facebook only (Warren, 2010). As Christine Warren states, “users need to assume that if [they] do something that is considered public, that action can potentially end up on a customized stream for everyone in [their] social graph”(Warren, 2010). Users need to know that they should be vigilant about protecting their privacy on-line and not just Facebook. The user needs to be confident that just because she has updated her Facebook profile saying that she is feeling down, she should not expect to receive e-mail solicitation for her to purchase Prozac.

Although, ultimately, the user is responsible for protecting her own privacy, she should have some measure of confidence that the protection of her privacy is a valued and measures taken to protect it. Otherwise the user may engage in privacy protecting behaviors that may be detrimental to usefulness of the data collected. One such behavior is misrepresentation of one’s identity. Consider the following example. One of my graduate students excitedly called me one day to tell me about her Facebook experience. Being concerned about her privacy, she had created a new Facebook profile for herself and purposely had given an erroneous birth date in which her aged was calculated to be 63. To her amazement, she recalled, that within hours she had received an e-mail from AARP (American Association of Retired Persons) inviting her to join that organization. Her misrepresentation of her age, nullifies any value that AARP would gained from knowing her age.

This is not a criticism of Facebook’s or any other company’s privacy policies per-se; it is intended to be a reminder of changing landscape of privacy and its impact on our daily lives. It is a call to action. No longer should we debate whether our privacy is in danger, it is time to assume that and seek ways to protect it. Companies should remember that a good privacy policy is good business and users should never assume that their privacy is protected. They need to become a more active participant in protecting their own privacy. In practice, information privacy deals with an individual’s ability to control and release personal information. The individual is in control of the release process: to whom information is released, how much is released and for what purpose the information is to be used. “If a person considers the type and amount of information known about them to be inappropriate, then their perceived privacy is at risk”(Roddick & Wahlstrom, 2001). Consumers are likely to lose confidence in the online marketplace because of these privacy concerns (Adkinson, et al, 1989; Milberg et al, 1995; Pitofsky, 2006; Smith et al, 1996). Business must understand consumers’ concern about these issues and aim to build consumer trust. It is important to note that knowledge about data collection can have a negative
influence on a customer’s trust and confidence level online. Privacy concerns are real and have profound and undeniable implications on people’s attitude and behavior (Sullivan, 2002). The importance of preserving customers’ privacy becomes evident when we study the following information: In its 1998 report, the World Trade Organization projected that the worldwide Electronic Commerce would reach a staggering $220 billion. A year later, Wharton Forum on E-commerce revised that WTO projection down to $133 billion. What accounts for this unkept promise of phenomenal growth? Census Bureau, in its February 2004 report states that “Consumer privacy apprehensions continue to plague the Web and hinder its growth.” In a report by Forrester Research it is stated that privacy fears will hold back roughly $15 billion in e-commerce revenue. In May 2005, Jupiter Research reported that privacy and security concerns could cost online sellers almost $25 billion by 2006. Whether justifiable or not, consumers have concerns about their privacy and these concerns have been reflected in their behavior. The chief privacy officer of Royal Bank of Canada said “Our research shows that 80% of our customers would walk away if we mishandled their personal information.”

**Information Security and Privacy Concerns of Medical uses of Information Technologies**

Another area of concern is the growth in the use of information technology for medical purposes. Confidentiality is sacrosanct in any physician-patient relationship and rules governing this relationship going back millennia are meant to protect patient’s privacy. Confidentiality, a major component of information security, is a significant mechanism by which a patient’s right to privacy is maintained and respected. However, in the era of Electronic Medical Record (EMR), it is hard to achieve. Although the use of information technologies for medical purposes shows potential for substantial benefits, it is fraught with concern related to security and privacy. Since there are so many points along the EMR life cycle where security and or privacy of medical data can be compromised, wide spread use of EMR is not possible without a thorough understanding and resolution of such issues (Amit, et al, 2005; Hunt, et. al, 1998; Johnston, et. al, 1994, Kensaku, et al, 2005). For example, Clinical decision support systems (CDSSs), an EMR based system, are designed to improve clinical and medical decision making and have been shown to improve healthcare practitioners’ performance and patient care (Amit, et al, 2005; Hunt, et. al, 1998; Johnston, et. al, 1994, Kensaku, et al, 2005). In a number of recent meta- analyses of several medical studies, it was reported that CDSS significantly improved clinical practice and medical decision making (Amit, et al, 2005; Hunt, et. al, 1998; Johnston, et. al, 1994, Kensaku, et al, 2005). One area of benefit that CDSS has shown considerable promise is in Comparative Effectiveness. Comparative Effectiveness (CE) simply means evaluating and comparing two or more possible treatments for a given medical condition in order to choose the best course of action. CE is nothing new and has been used to enhance the practice of medicine for centuries. Comparative effectiveness have successfully been applied in numerous areas of medical diagnosis and treatment, including selection of the most favorable medication among competing drugs, deciding on the use of the most efficacious medical procedures or devices, and the use of best clinical treatment management. The non-partisan Congressional Budget Office (CBO) estimates that nearly $700 billion each year goes to health-care spending that can’t be shown to lead to better health outcomes. The use of comparative effectiveness can help mitigate this problem. Studies have shown that the use of comparative effectiveness improves clinical care while reducing medical costs. This can benefit insurance providers, employers, government and patients. CBO suggests that the use of comparative effectiveness of clinical care provides the best op-
portunity to constraint the runaway medical cost and could result in substantial reduction of the overall cost of care without sacrificing the quality of care (Please See CBO’s Pub. No. 2975, 2007). Realizing the importance of CE, in 2008 legislation was introduced in Congress that established the Health Care Comparative Effectiveness Research Institute as an ambitious program to study how to achieve the best clinical outcome for patients with minimal cost. Comparative effectiveness studies make extensive use of retrospective analysis of patient data. Retrospective analysis of patient data has contributed to advancement of the art and science of medical decision making for a long time (Lavarac 1999). Retrospective analysis of patient data has contributed to advancement of the art and science of medical decision making (Lavarac 1999). Given the current pace of advancement in medicine there is a great need to develop computer assisted medical decision making systems based on retrospective analysis to enhance and support the practice of medical decision making. Such systems need to learn the decision characteristics of the diseases before they can be used to diagnose future patients with uncertain disease states (Van Bemmel, 1997). To achieve this goal, the system needs to be presented with high quality, non fragmented historic patient data as the fundamental ingredient of robust analysis. However, using patient data for retrospective analysis in support of medical decision making poses a number of significant security and privacy challenges when considering that most patient data, at the time of collection, were intended for patient care and may not have been explicitly collected for research purposes. Security and privacy concerns using retrospective analysis of medical data for comparative effectiveness are too numerous to mention involve many complex technical and non technical issues that need to be resolved before the use of such systems can become wide spread. These challenges stem from the fact that patient data sets are large, complex, heterogeneous, hierarchical, time series, nontraditional, and originate from a verity of sources with differing levels of quality and format. Further, data sources may have incomplete, inaccurate and missing elements, some may be erroneous due to human and equipment error and lastly, the data may lack canonical consistencies within and between sources (Ciosa, et al, 2002). Patient data are voluminous and are collected from various sources including medical images, patient interviews, laboratory data, and the physicians’ observations and interpretations of patients’ symptoms, and behavior (Ciosa, et al, 2002). Securing such diverse and voluminous type of data residing on multiple heterogeneous systems with diverse data stewardship is not a trivial task and requires a whole set of different and difficult considerations. For example, medical data lack the underlying data structures needed for mathematically based data encryption techniques. Unlike data collected using other processes, medical data consists of word descriptions by physician and nurses, with very few formal constraints on the vocabulary, medical images, hand written charts and others. Additionally, medical data also lack a canonical form that encapsulates all equivalent forms of the same concept and is the preferred notation used in most encryption algorithms. For example, all the following are medically equivalent: Colon adenocarcinoma, metastatic to liver; Colonic adenocarcinoma, metastatic to liver; Large bowel adenocarcinoma, metastatic to liver. (Ciosa, et al, 2002). Lastly, medical data are time sensitive and may have been collected at different times using different data collection methodologies. As a result, they may reside on heterogeneous systems with differing representation and stewardship. Massive quantities of patient data are generated as patients undergo different medical and health care processes and procedures. As a result, these large patient databases may contain large quantity of useful information about patients and their medical conditions, possible diagnoses, prognosis and treatments. A major challenge in using these large patient databases is the ability to properly secure and anonymize the data. Another security and privacy issue deals with data mining of medical data. Careful and systematic mining of patient databases may reveal and lead to the discovery of useful trends, relationships and patterns that could
significantly enhance the understanding of disease progression and management. This process is referred to as Data mining (DM). DM is an exciting new facet of decision support systems. Data mining derived from the disciplines of artificial intelligence and statistical analysis and covers a wide array of technologies. Using data mining, it is possible to go beyond the data explicitly stored in a database to find nontrivial relationships and information that would not have been discovered by way of standard analysis methods. Medical Data Mining (MDM) is data mining applied to patient data and has been shown to provide benefits in many areas of medical diagnosis, prognosis and treatment (Lavrac, 1999; Prather, et. al, 2009; Rayward-Smith et.al 2001; Wang et al, 2000). By identifying patterns within the large patient databases, medical data mining can be used to gain more insight into the diseases and generate knowledge that can potentially lead to development of efficacious treatments. Unfortunately, given the difficulties associated with mining patient databases, the potential of these systems are yet to be realized (Lavrac, 1999; Prather, et. al, 2009; Wang et al, 2000). Medical Data Mining is the process of discovering and interpreting previously unknown patterns in medical databases (Lavrac, 1999; Prather, et. al, 2009; Wang et al, 2000). It is a powerful technology that converts data into information and potentially actionable knowledge. However, obtaining and using new knowledge in a vacuum does not facilitate optimal decision making in a medical setting. In order to develop a successful final patient treatment management, the newly extracted useful medical knowledge from MDM that appears in form of relationships and patterns should be integrated with existing knowledge and expertise that of the physician to enhance patient care. The significance of data security and privacy has not been lost to the data mining research community as was revealed in Nemati and Barko (Nemati et al., 2001) of the major industry predictions that are expected to be key issues in the future (Nemati et al., 2001). Chiefly among them are concerns over the security of what is collected and the privacy violations of what is discovered ((Margulis, 1977; Mason, 1986; Culnan, 1993; Smith, 1993; Milberg, S. J., Smith, & Kallman, 1995), and (Smith, Milberg, & Burke, 1996). One of the most far reaching laws with privacy implication impacting medical data mining research and practitioner communities is Health Insurance Portability and Accountability Act of 1996. It provides a standard for electronic health care transactions over the Internet. As the integrity and confidentiality of patient information is critical, this requires being able to uniquely identify and authenticate an individual. Health information is subject to HIPPA. The original legislation went into effect in 2001 and the final modifications took effect in April, 2003. A core aspect of HIPAA is to appropriately secure electronic medical records. The act applies to health information created or maintained by health care providers who engage in certain electronic transactions, health plans, and health care clearinghouses. The Office for Civil Rights (OCR) is responsible for implementing and enforcing the HIPPA privacy regulation. HIPAA has strict guidelines on how healthcare organizations can manage private health information. This includes: Authentication: A unique identification for individuals using the health care system; Access control: Manage accounts and restrict access to health information; Password management: Centrally define and enforce a global password policy; Auditing: Centralize activity logs related to the access of health information. The act sets standards to protect privacy in regards to individuals’ medical information. The act provides individuals access to their medical records, giving them more control over how their protected health information is used and disclosed, and providing a clear avenue of recourse if their medical privacy is compromised (Anonymous, 2006). Improper use or disclosure of protected health information has the potential for both criminal and civil sanctions. For example, fines up to $25,000 for multiple violations of a single privacy standard in a calendar year and the penalties for intentional or willful violations of the privacy rule are much more severe with fines up to $250,000 and/or imprisonment up to 10 years for knowing misuse of personal health data. There are more immediate risks of private lawsuits relying on the HIPAA standard of care.
Implications of Information Security and Privacy

A common motivation for corporations to invest in information security is to safeguard their confidential data. This motivation is based on the erroneous view of information security as a risk mitigation activity rather than a strategic business enabler. No longer should information security be viewed solely as a measure to reduce risk to organizational information and electronic assets, it should be viewed as way the business needs to be conducted. To achieve success in information security goals, it should be organization information security should support the mission of the organization. The Information Systems Security Association (ISSA) has been developing a set of Generally Accepted Information Security Principles (GAISP). GAISP include a number of information security practices including the need for involvement of top management, the need for customized information security solutions, need for periodic reassessment, the need for an evolving security strategy and the need for a privacy strategy. This implies that it should be viewed as an integral part of the organizational strategic mission and therefore, it requires a comprehensive and integrated approach. It should be viewed as an element of sound management in which the cost-effectiveness is not the only driver of the project. Management should realize that information security is a smart business practice. By investing in security measures, an organization can reduce the frequency and severity of security-related losses. Information security requires a comprehensive approach that extends throughout the entire information life cycle. The management needs to understand that without a physical security, information security would be impossible. As a result, it should take into considerations a variety of issues, both technical and managerial and from within and outside of the organization. The management needs to realize that this comprehensive approach requires that the managerial, legal, organizational policies, operational, and technical controls can work together synergistically. This requires that senior managers be actively involved in establishing information security governance.

Effective information security controls often depend upon the proper functioning of other controls but responsibilities must be assigned and carried out by appropriate functional disciplines. These inter-dependencies often require new understanding of the tradeoffs that may exist, that achieving one may actually undermine another. The management must insist that information security responsibilities and accountability be made explicit and the system owners have responsibilities that may exist outside their own functional domains. An individual or work group should be designated to take the lead role in the information security as a broad organization wide process. That requires that security policies be established and documented and the awareness among all employees should be increased through employee training and other incentives. This requires that Information security priorities be communicated to all stakeholders, including, customers, and employees at all levels within the organization to ensure a successful implementation. The management should insist that information security activities be integrated into all management activities, including strategic planning, capital planning. Management should also insist that an assessment of needs and weaknesses should be initiated and security measures and policies should be monitored and evaluated continuously.

Information security and privacy professionals are charged with protecting organizations against their information security vulnerabilities and privacy threats. Given the importance and securing information to an organization, this is an important position with considerable responsibility. It is the responsibility of information security professionals and management to create an environment where the technology is used in an ethical manner. Therefore, one cannot discuss information security without discussing the
ethical issues fundamental in the development and use of the technology. According to a report by the European Commission (EC, 1999, p. 7) “Information Technologies can be and are being used for perpetrating and facilitating various criminal activities. In the hands of persons acting with bad faith, malice, or grave negligence, these technologies may become tools for activities that endanger or injure the life, property or dignity of individuals or damage the public interest.” Information technology operates in a dynamic environment. Considerations of dynamic factors such as advances in new technologies, the dynamic nature of the user, the information latency and value, systems’ ownerships, the emergence of a new threat and new vulnerabilities, dynamics of external networks, changes in the environment, the changing regulatory landscape should be viewed as important. Therefore the management should insist on an agile, comprehensive, integrated approach to information security and privacy.

David Mackey, IBM’s Director of security intelligence estimates that IBM recorded more than 1 billion suspicious computer security events in 2005. He estimates that a higher level of malicious traffic in 2006. The damage from these “security events” can range from lose of integrity of the information to total physical destruction or corruption of entire infrastructure that support it. The damages can stem from the actions of a variety of sources, such as disgruntle employees defrauding a system or careless errors committed by trusted employees to hackers gaining access to the system from outside of the organization. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are “swept under the carpet” to avoid unfavorable publicity. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system. Broadly speaking the main purpose of information security is to protect an organization’s valuable resources, such as information, hardware, and software.

The importance of securing our information infrastructure is not lost to the government of the United States. The US Department of Homeland Security (DHS) identifies a Critical Infrastructure (CI) as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” According a recent report by the DHS titled The National Strategy for Homeland Security, which identified thirteen CI’s, disruption in any components of a CI can have catastrophic economic, social and national security impacts. Information Security is identified as a major area of concern for the majority of the thirteen identified CI’s. For example, many government and private-sector databases contain sensitive information which can include personally identifiable data such as medical records, financial information such as credit card numbers, and other sensitive proprietary business information or classified security-related data. Securing these databases which form the back bone of a number of CI’s is of paramount importance. Losses due to electronic theft of information and other forms of cybercrime against to such databases can result in tens of millions of dollars annually.

In addition to specific costs incurred as the results of malicious activities such as identity theft as a result of data breaches such as theft of hardware or system break ins, or virus attacks or denial of service attacks, one of the major consequences of dealing with a security attacks are the decrease in customer and investor confidence in the company. This is an area of major concern for the management. According to an event-study analysis using market valuations done by (Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan, 2004) to assess the impact of security breaches on the market value of breached firms, announcing a security breach is negatively associated with the market value of the announcing firm. The breached firms in the sample lost, on average, 2.1 percent of their market value
within two days of the announcement—an average loss in market capitalization of $1.65 billion per breach (Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan, 2004). The study suggests that the cost of poor security is very high for investors and business. Financial consequences may range from fines levied by regulatory authorities to brand erosion. As a result, organizations are spending a larger portion of their IT budget in information security. A study by the Forrester Research Group estimates that in 2007 businesses across North America and Europe will spend almost 13% of their IT budgets on security related activities. The same report shows the share of security spenditure was around 7% in 2006.

CONCLUSION

It is obvious that information security and privacy are top priorities for society, as they should be. Regardless of the source, the impact of a security breach or a privacy threat on an organization, either private or governmental, can be severe, ranging from interruption in delivery of services and goods, to loss of physical and other assets, to loss of customer good will and confidence in the organization. Such breaches or privacy threats to sensitive data can be very costly to an organization. Recent research shows that investing and upgrading information security and privacy infrastructure is a smart business practice. By doing so, an organization can reduce the frequency and severity of losses resulted from security breaches in computer systems and infrastructures. Information is a critical asset that supports the mission of an organization. Protecting this asset is critical to survivability and longevity of any organization. Maintaining and improving information security is critical to the operations, reputation, and ultimately the success and longevity of any organization. However, Information and the systems that support it are vulnerable to many threats that can inflict serious damage to organizations resulting in significant losses. The concerns over information security risks can originate from a number of different security threats. They can come from hacking and unauthorized attempts to access private information, fraud, sabotage, theft and other malicious acts or they can originate from more innocuous sources, but no less harmful, such as natural disasters or even user errors.

Information Security and privacy are not just technological issues alone. They encompass all aspects of business from people to processes to technology. Bruce Schneier founder and editor of Schneier.com states that “If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.” Information Security and privacy involve consideration of many interrelated fundamental issues. Among them are technological, developmental and design, and managerial considerations. The technology component of information security and privacy is perhaps the easiest to develop and to achieve. The technological component of information security and privacy is concerned with the development, acquisition, and implementation of hardware and software needed to achieve security and privacy. The developmental and design component of information security and privacy deals with issues related techniques and methodologies used to proactively development and design systems that are secure and private. The managerial and personnel component focuses on the complex issues of dealing with the human elements in information security and privacy. They deal with policies, procedures and assessments required for the management of the operation of security and privacy activities. Undoubtedly, this is the hardest part of the information security and privacy to achieve since it requires a clear commitment to security and a culture of valuing privacy by the organizational
leadership, assignment of appropriate roles and responsibilities, implementation of physical and personnel security and privacy protecting measures to control and monitor collection and access to data, training that is appropriate for the level of access and responsibility, and accountability. Privacy consideration is an important antecedent to developing a customer’s intention to engage with a web site for commercial, informational or entertainment purposes. As a result, privacy has become an import business driver. Studies have shown that when people (customers) feel that privacy is ‘violated’, they respond to it in different ways with different levels of intensity (Culnan, 1993). Still, despite this divergent and varied reaction to privacy violation, or maybe because of it, a lot of companies still do not appreciate the depth of consumer feelings and the need to revamp their privacy practices, as well as their infrastructure for dealing with privacy. Privacy is no longer about just staying within the letter of the latest law or regulation. Sweeping changes in the attitudes of people about their privacy fueled by their privacy fears will cause an intense political debate and will put once-routine business and corporate practices under the microscope, resulting in a patchwork of regulations not favoring businesses. Regulatory complexity will grow as privacy concerns surface in scattered pieces of legislation (Anonymous, 2006). Companies need to respond quickly and comprehensively. They must recognize that privacy should be a core business issue. Privacy policies and procedures that cover all operations must be enacted. Privacy Preserving Identity Management should be viewed as a business issue, not a compliance issue.

Advances in IT have allowed people to transcend the barriers of time and geography and to take advantage of opportunities not even conceivable today, opening up a new world of possibilities and opportunities. The IT revolution has transformed our lives in way unimaginable only a decade ago. Yet, we are only at the threshold of this revolution. The dizzying pace of advances in information technology promises to transform our lives even more drastically. In order for us to take full advantage of the possibilities offered by this new interconnectedness, organizations, governmental agencies, and individuals must find ways to address the associated security and privacy implications of their actions and behaviors. As we move forward, new security and privacy challenges will likely to emerge. It is essential that we are prepared for these challenges.

REFERENCES


Mason, R. O. (1986). Four ethical issues of the information age. MIS Quart., 10(1), 4-12.


