Best Practices for Protecting Consumer Data

Jillena Locklear
ICTN 6823 Information Security Management
7/9/2014

Table of Contents

Introduction

The field of information technology (IT) has grown extensively in the past few decades. This growth can be attributed to the advancement of technology and the impact that new technology has had on consumerism. Technology has developed a new avenue for societal consumers. The World Wide Web (Internet) alone has paved the way for consumers to enjoy the comforts of their home and make purchases online avoiding the hustle and bustle of common crowds at malls and other various retail centers. Other aspects of online technology including e-mail, search engines, applications (apps) and social media, all play a role in collecting information from users. These forms of online activities are popular among consumers and are used daily to retrieve and send vital information. Most of the time, the information that is shared using these various tools is personal and can contain information relating to location of user, banking information, birthday, social security numbers, telephone numbers, etc. There is a saying that is commonly heard among the information technology field that says, "Once it is put on the Internet, it cannot be completely removed." This highlights the fact that information that is shared to online websites is digitally sealed.

Therefore it is inevitable that from a perspective of information technology, data that is collected from online consumers must be regulated and protected. This upholds privacy of individuals, which is constitutionally protected. There are various avenues one can take to protect consumerism in this highly digital age, and this paper will address these ways and offer recommendations and possible solutions that can be implemented. In addition, enforcement of these regulations is key to successful integration, so the government, specifically the Federal Trade Commission (FTC), can play a critical role in enforcing potential protective techniques. The paper will illustrate how pertinent

consumer data protection is to the field of information technology and how IT professionals can begin to protect information consumers share about themselves across various servers and networks.

Consumerism in a Digital Age

Consumerism has evolved through a radical process based on an ever-progressing technological society. In the past, consumerism was only available to individuals who physically visited retail stores and made purchases. However, today that ancient age of consumerism is a part of history. The development of computing technology (mobile and stationary) as well as e-mail, online transactions and social media has opened a digital world allowing consumers and individuals to access accounts with the input of a username and password. Many accounts consumers access across e-mail domains and web pages utilize this same username and password technique. This technique is used by online consumer webpages where individuals can make purchases with their account as well as social media domains where individuals share and post pictures and other personal data. Also, educational systems employ the username and password technique specific to each student. With the input of a username and password, individuals can share masses of information. This large mass of information shard by a consumer is gathered by these online companies. The boundaries of online consumerism is not just limited to these previously mentioned entities, but include numerous more such as students applying for federal aid online, completing taxes, completing job applications, the boundaries are plentiful. All of these are examples of online accounts that collect and store data shared through consumers or individuals who input personal information.

Why do these companies continue to gather and process information shared by their users? A report published in 1997, when these advancements were really beginning to catch on indicated that companies can effectively pinpoint what they continue to offer to specific customers. For example, based on recent searches gathered from a search engine, the company can tailor future searches that accompany recent searches conducted by the customer. This is also true for online retailers. Evidence shows that by doing so, customers are more satisfied with their experience. Also, collected information can generate new ideas and services that can be allotted to consumers. (Hagel III & Rayport, 1997).

The Apple Company calls their digital storing area, "The Cloud." Inside the cloud lies previous transactions purchased by consumers. In the field of IT, online markets do not have a fancy term such as Apple that stores previous information and personal data. Instead, physical data gathered from consumers is transferred to an electronic database. This information is sometimes shared with outside parties for various reasons. For example, governmental agencies (federal, state and local) collect consumer information such as address, birthday, marriage, property information, vehicle registration, and parenthood, number of individuals living in a household, salaries, and even death records. (Nissenbaum, 1998). According to an article written by a professor at Princeton University, consumers who share information online are characterized by personal identification numbers gathered through online sharing of information. It is argued that, "…people are identified through name, address, phone number, credit card numbers, social security number, passport number and more" (Nissenbaum, 1998, p. 561). This is

vital personal information that when shared with the wrong individual or party, can be detrimental to an individual's personal life; not just financially but also physically.

One key factor that is critical to digital data consumerism is consumer trust. Without trust, consumers will not access any of these online consumer markets. To retain consumer use, online retailers, e-mail servers, social media networks and online banking institutions, must maintain privacy trust from consumers or they will lose clients. In a survey that was conducted by Business Week in the year 2000, it was reported that 61% of respondents identified that they would engage in Internet transactions if they could conclude that their personal information shared via the web was protected. (Chellappa & Pavlou, 2002).

Most consumers share information across various networks assuming that the information they are sharing is protected. Some assumptions are based upon the belief that many of these networks and domains must follow statutes put into place by the government, specifically the FTC. This assumption is mostly true. A report released by the United States White House (2012) suggested that the "framework" for data protection in the US in indeed strong. The current framework consists of "…fundamental privacy values, flexible and adaptable common law protections and consumer protection statues, Federal Trade Commission (FTC) enforcement, and policy development that involves a broad array of stakeholders" (The White House of the United States, p. i). These methods may be a strong framework for protecting consumer data, but this current framework needs to be added unto to strengthen security and to maintain consumer trust. This digital age of consumerism is not slowing down. Professionals in the field of IT and other

governmental bodies and agencies need to act with haste concerning the issue of protecting the privacy of the public.

Privacy and Consumer Data: The Problem

Privacy and consumer data shared via online domains and networks continues to be a main threat to the public at large. With the assumption of trust, many consumers who continue to utilize online markets become targets of prey to online predators who constantly develop ways of hacking systems to gather information. Companies may issue policy statements that address the right to privacy for consumers, stating that personal consumer information will not be shared with a third party. However, these policy issues are useless in the occurrence of a security breach when hackers break into systems stealing consumer information useful to their personal gain.

These forms of security breaches are present in just about every online public market in existence. Consumers are urged by retailers, government agencies, educational institutions and other companies to conduct their business online. These agencies ensure that their protection is safeguarded. Ultimately, these companies speak of ease, speed and the affordability of conducting such personal business through the online market. (Nissenbaum, 1998), This type of behavior has allowed for additional growth of online consumerism. In fact, the government collects various information from online consumers. Nissenbaum suggested in her article (1998) that hackers are not the only collectors of personal information shared by consumers. Government collects information and in certain cases electronically releases it when necessary or in instance when commanded to do so by the justice system in the need of evidence during a case hearing. The government denies releasing personal information, but it is done so in certain cases

like previously described. This type of information sharing is beginning to be noticed by the public and other IT professionals and policymakers. These populations are declaring that this type of information attainment is unnecessary and "illegitimate". (Nissenbaum, 1998). This issue is beginning to take form as the problem worsens and progresses. Current events such as the leak of private information and network security breaches occurring in the news lately, are shining light on the issue and the public are more aware of the dangers of consumer data collection.

Consumers strongly believe in their privacy rights. The ease, accessibility and speed of technological consumerism is attractive and popular among all generations of life, but when privacy and personal information is at stake, it negates the latter. Consumers want to enjoy the benefits of online consumerism markets, but refuse to put their personal security at risk. It is suggested that the knowledge of online markets collecting and storing data about an individual is alone difficult to deal with. However, when coupled with sharing information with other outside parties without consent infringes upon their rights to privacy; therefore adding fuel to the fire. (Nissenbaum, 1998). To address this public issue of privacy and consumer data, IT is critical in developing alternatives as solutions and integrating them into these online markets to improve security and protect consumers. As you can imagine, current literature offers a vast array of possible solutions. These solutions come in different packages ranging from actual technological developments to policy and consumer awareness techniques. Each possible solution to be discussed holds its own place as a noteworthy candidate of success in alleviating the matter at hand.

Notable Techno Alternatives for Protecting Consumer Data

These prospective proposals to be discussed can serve as blueprints in the field of IT. Computer specialists, technology professionals, public policy officials and governmental bodies can gain an edge in alleviating this issue of public privacy in online markets by examining these recommended methods. First, the mind subconsciously appeals to creating savvy techno mechanisms that are geared to protecting consumer data. In fact, this is an excellent potential remedy for the problem. Since the problem continues to grow, many professionals in their field have explored the idea of developing techno gadgets to be implemented in IT for data protection. Many of these ideas have been put to the test and prove their worth and meaningfulness.

A report released by an IT company giant that thrives on security, offered best practices for online privacy. The company recommended sticking to common mechanisms of security currently used, but beefing them up for added security. The company also suggests implementing other technological gizmos warranted to protect privacy of consumers. It is beneficial to mention that the report was suggested for mobile and remote machines. However this pertains to all online markets. Currently it is required that remote machines follow established protocols and policies that are enforced by corporate retailers and companies. One is maintaining the latest version of antivirus software. This software is crucial to detecting any intrusion attempt into a network and transferring data of consumers. Tools are already in existence that identify any vulnerabilities in networks. These network based assessment tools exist in VPN gateways and can spot ports that are a threat to a possible security breach. In addition these tools can examine machines when they come in contact with the network and determine if the

machine is safe enough to access the network. (Beyond Trust Software Inc, 2013). This is a primary mechanism to protect data consumer privacy by detecting potential threats and nipping them before they occur. Also another tool called, host-based vulnerability assessment tools, are implanted onto the remote and mobile device itself. This tool scans files and the software of the device and identifies any vulnerabilities based upon permissions to access information not given by the correct body. (Beyond Trust Software Inc, 2013)

In addition to the common and current techniques, Beyond Trust went a step further to introduce a few new technological tools. The company recommends to implement some sort of an intrusion prevention technology. This tool can examine the traffic on the network and access the devices and determine if they are complaint to the networks enforced policies and protocols concerning privacy. It is proposed that the tool compare its findings to a database that is frequently updated with the known and most popular attacks used to hack into information storage systems. (Beyond Trust Software Inc, 2013). A scanner that is connected to the host machine or the host network will remotely scan its system to ensure that it is operating as suspected. Based upon these mechanisms discussed above, Beyond Trust developed a system given the name Retina Endpoint Intrusion Prevention that will identify and protect devices from vulnerability to online predators. Retina incorporates old technology including antivirus software, firewalls, anti-spyware, and anti-phishing and beefs it up with the addition of the vulnerability scanner. This protects the mobile devices and host network from unwanted attack. The performance of the Retina is operated by scheduled maintenance windows that access systems. It does not rest in dormant mode waiting for an intrusion attempt to

occur. It also incorporates maintaining compliancy to network safety protocols, knocking out devices that cannot comply due to outdated software or other potential security threat. (Beyond Trust Software Inc, 2013) As you can see, this company has offered some wonderful technological recommendations and even a device that can be implemented to protect consumer data. But there are others that are just as useful.

In Europe, IT professionals have developed tools that have been successful in protecting network and consumer data protection. The first is referred to as a System Logger (SysLog). This tool has been tested and utilized in UNIX operating systems. (Saitovic & Ivanovic, 2011). The SysLog examines the current operation of the system. It collects messages on a central server. This enables the system to easily manage the performance of the network. There is one problem with using the SysLog system. It only operates effectively with the transport layer protocol. The application layer is left unattended, so there are issues as to whether messages are delayed to their proper destination. These messages can contain possible system intrusion data. Whatever the case, it is one of the most widely used tools for regulating system and network performance. (Saitovic & Ivanovic, 2011). The SysLog system contains some internal process that are unique to its application. First, the SysLog indicates the origin of the message. In essence, it determines what part of the system is detecting an issue. Secondly, the severity of the issue is indicated and relayed to the systems manager or host. (Saitovic & Ivanovic, 2011) This system has proved its longevity and usefulness in maintenance of networking systems. It is a widely trusted technique allowing for security and protection of data and information contained on a specific domain or network.

Previously mentioned, Beyond Trust recommended that networks install a traffic protocol to routinely monitor the flow of traffic utilizing the network. This can be one of the quickest and easiest ways of detecting a security threat before it attempts an attack. The NetFlow protocol was developed by Cisco Systems Inc. to serve as their devices traffic monitor. (Saitovic & Ivanovic, 2011). This protocol manages the flow of traffic on the network called the network load and assesses the "nature" and "services" commonly utilized by the traffic. (Saitovic & Ivanovic, 2011). NetFlow intermittently evaluates the traffic and collects data and statistics which is communicated to the network server. Most of the data is communicated via tables, graphs and other graphical interpretations. This protocol can detect system viruses, traffic abuse, unrestricted access, intrusion attempts, and any unwarranted open ports that may exist on the network. (Saitovic & Ivanovic, 2011). This protocol is another current tool used by tech giants that may be beneficial for IT professionals to utilize as a solution to protecting consumer data.

One last article published in Harvard Business Review (2013) suggested that a certain device be developed to act much like data collection devices used by online consumer markets. Indeed it is true as mentioned earlier, that consumers are more satisfied with services and networks that can tailor suggestions based on their account activity. Therefore the authors suggest why not building off of this success and developing Choice Engines. Choice Engines are smart engines that collect consumer data and utilizes it to tailor services specific to consumer. Unlike data collection today, Choice Engines allow for consumers to access data that is collected on them to understand its usefulness and strategy behind its tactic. (Thaler & Tucker, 2013). This establishes trust with the consumer and also allows for continued growth of online markets and

businesses. Choice Engines can decipher information and output services that will be most beneficial to consumers.

For example, banks can utilize Choice Engines when determining a mortgage for a certain couple. The Choice Engine can gather salary, social security, job information data and credit history, process it and output a mortgage just perfect for the couple. A mortgage that will not become a financial burden for the couple for years to come. The authors also suggest its use in everyday activities such as grocery shopping. Choice Engines can gather recent and frequent purchases and output coupons and specials on the products they need and use often. It can even be tailored to know when an individual will require a restock of certain grocery products and notify them via e-mail text, social media, or other form of digital communication. (Thaler & Tucker, 2013). The drawback for this innovate idea is cost. Implementing such a technological device will be costly. So policymakers will need to address smart information disclosure options to allow consumers to gain access to their data and continue to prevent third party hackers. (Thaler & Tucker, 2013)

Non-Tech and Policy Recommendations for Consumer Data Protection

Besides these various technological devices and systems to integrate into networks and online markets for consumer data protection, many have regarded that policy recommendations and laws are secure ways of data protection as well. According to an article published in IASSIST Quarterly (1998), the U.S. does not have any specific laws that govern privacy when it comes to data collection. There are laws in place that monitor the government's collection and use of personal data. These include the Privacy Act of 1974 and the Computer Matching and Privacy Act. (Stratford & Stratford, 1998).

Government has procrastinated the idea of protecting consumer data collection outside of government hands. It could be worthwhile to the IT field that government lends a hand and develops laws to govern data collection in the private and public sectors not affiliated with the government such as online retailers and e-mail servers.

In fact a couple of authors and computer science professionals from the Massachusetts Institute of Technology agree that in order to protect large masses of data collection, laws must be orchestrated and implemented to govern use. The authors illustrate how laws and policy protocols can maintain large scale data collection. These examples included the Fair Credit Reporting Act utilized by private credit systems and Securities Law which regulates public companies financial standing guarded by the Securities and Exchange Commission (SEC). These policy protocols have succeeded in control and maintenance of large scale information collected from company networks. (Weitzner, et al., 2007). It is suggested by the authors that development of such policy protocols can come in the existence of policy aware transaction logs and policy reasoning tools. Transaction logs will regulate and ensure that collected information has been done so according to policies that have been embedded into the network framework. These polices will act as accountability for the network allowing for privacy compliancy to consumers. Reasoning tools can determine if certain information collected is indeed useful to the company. If so, the reasoning tool will either collect the data deemed useful or disregard it. This ensures that only pertinent data needed is stored by the network and unwanted personal data is privately secured by the consumer only. (Weitzner, et al., 2007). These are interesting theories and tools that can serve as potential solutions to

protecting consumer data. Instead of using fancy technological gadgets, network security frameworks can be constructed based on policies and procedures.

Conclusion and Discussion

Due to the heavy volume of public privacy issues, the U.S. has decided to begin developing possible solutions by policy regulation. The FTC has issued a recent report (2014) that details how laws have been utilized by the commission to settle cases that have occurred dealing with privacy and protection. Current Laws including the Fair Credit and Reporting Act (FCRA), Gramm-Leach-Biley Act (GLB Act) and the Children's Online Privacy Protection Act (COPPA) have been reorganized, added to and utilized to enforce statues and rules that the commission has set into place. (The Federal Trade Commission, 2014). In a recent case concerning the "Internet of Things" the commission used these laws to settle the case that involved TRENDnet which uses SecurView cameras to monitor daily activities that occur in a consumer's home. (The Federal Trade Commission, 2014). This was used in home security systems and baby monitoring systems. The recorded videos were leaked to outside parties and were visible to online viewers. Thankfully, the commission was able to settle damages expressed in the case. The report also concluded that the commission will continue to undertake policy initiatives to enforce security outside of governmental boundaries. (The Federal Trade Commission, 2014).

A key role in protecting consumer data is to educate consumers. Consumers require education on security of their mobile and stationery devices to ensure that when conducting consumerism in online markets and networks, their device is protected from hackers who try to tap into it and steal information. This is critical because host networks

are not the only place where consumer data can be collected from, personal devices is also a major target. The FTC is making progress in this aspect of consumer data protection as well. (The Federal Trade Commission, 2014). As an IT student and professional, I urge that these practices continue by the FTC and that other security companies and IT professionals take an interest in developing tools as discussed in this paper to protect consumer data. Also policymakers and government must continue to play a role in this issue. Policy can issue enforcement and accountability for public and private markets who collect consumer data. As society continues to progress, so will technology. I am certain that this issue will continue to be prevalent, so therefore this paper offers some wonderful suggestions and prospects for gaining trust of consumers and safeguarding their privacy.

References

Beyond Trust Software Inc. (2013). *Best Practices for Securing Remote and Mobile Devices.* Phoenix: Beyond Trust.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions. *Logistics Information Management, 15*(5/6), 358-368.

Hagel III, J., & Rayport, J. F. (1997). The Coming Battle for Customer Information. *The McKinsey Quarterly*(3), 65-76.

Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy, 17*, 559-596.

Saitovic, E., & Ivanovic, I. (2011). *Network Monitoring and Management Recommendations.* Amsterdam: Terena.

Stratford, J. S., & Stratford, J. (1998). Data Protection and Privacy in the United States and Europe. *IASSIST Quarterly*, 17-20.

Thaler, R. H., & Tucker, W. (2013). Smarter Information, Smarter Consumers. *Harvard Business Review*, 45-54.

The Federal Trade Commission. (2014). *Protecting Cinsumer Information: Can Data Breaches Be Prevented.* Washington: United States House of Representatives.

The White House of the United States. (2012). *Consumer Data Privacy In A Networked World: A Framework For Protecting Privacy And Promoting Innovation In The Global Digital Economy.* Washington: The White House.

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2007). *Information Accountability.* Cambridge: Massachussetts Institute if Technology.