JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Volume 11, Issue 2
August 2018
ISSN: 1946-1836

In this issue:

iscap Information Systems & Computing Academic Professionals

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer-reviewed academic journal published by **ISCAP,** Information Systems and Computing Academic Professionals. Publishing frequency is three issues a year. The first date of publication was December 1, 2008.

JISAR is published online (http://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (http://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of AITP-EDSIG who perform the editorial and review processes for JISAR.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

2018 JISAR Editorial Board

Information Security and Privacy Legislation: Current State and Future Direction

Lex Dunlap
ad4991@uncw.edu

Jeff Cummings
cummingsj@uncw.edu

Thomas Janicki
janickit@uncw.edu

Department of Business Analytics, Information Systems and Supply Chain
University of North Carolina Wilmington
Wilmington, NC 28403

Abstract

The field of information security and privacy is continually growing and evolving to meet the needs of both individuals and organizations. While individuals may still struggle securing their own data, organizations must follow specific regulations concerning any data they hold that is considered private (e.g., social security number, driver's license number, etc.). However, the challenge for most organizations is understanding those regulation as they exist at both the federal and state level. Complicating matters further is the fact that laws may differ from state to state. The current research examines the security and privacy landscape that organizations must navigate. The goal is to get a better understanding of federal and state security/privacy laws while discussing future directions that should be taken at both levels to ensure the privacy and security of an individual's data.

Keywords: Information Security, privacy, regulation, laws

1. INTRODUCTION

Information security and privacy issues continue to dominate the news such as the recent WannaCry ransomware which has attacked over 200,000 computers in 150 countries (Sherr, 2017). These types of attacks target both businesses and consumers alike, emphasizing how quickly an individual's data may be compromised. Additionally, with the recent passage of legislation enabling Internet Service Providers (ISPs) to collect and disseminate customer information, the need for organizations to understand privacy continues to increase (Washington Post, 2017). Businesses, institutions, and customers alike need to consider how sensitive data is being managed. For companies, this requires not only an understanding of security methods necessary for maintaining data, but also the regulations and requirements organizations are legally bound to uphold.

The National Institute of Standards and Technology (NIST) defines information security as "the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Nieles, Dempsey and Pilliteri, 2017, p.2)." This research is concerned with confidentiality or "preserving authorized restrictions on information access and disclosure, including means of protecting personal privacy and proprietary

information (Nieles et al. 2017, p.2)." Each company is required to adhere to the laws that are applicable to their corporation and the states in which they conduct business. This means each company must understand the laws that exist at both the federal and state levels. While there are some federal laws regarding the security of specific types of data (e.g., medical information or financial information), organizations often struggle to understand how to keep individual data secure as many of these laws vary based on the location of the company and the individual. Surprisingly, most security and privacy laws remain at the state level making organizational compliance daunting as states may have varying laws. The goal of this research is to get a better understanding of the current state of security and privacy laws in the US while providing some suggestions for future directions. In the following sections, we examine the varying viewpoints of what is "private data" and how current federal regulations impact organizations. In addition, a discussion of security and privacy laws at the state level will occur to understand how private information is handled from state to state. We conclude with a discussion of the possibilities moving forward and potential changes that may help with consumer data privacy. This research reflects the viewpoint of the information held by companies on individuals and not on the data held by individuals on themselves.

2. CURRENT SECURITY AND PRIVACY LAWS

Currently, laws and regulations regarding security and privacy of an individual's information exists at both the federal and state level. While most laws have been passed at the state level, we will discuss both levels in the following sections. However, we first discuss the idea behind what is considered private data to provide better context to the discussion surrounding laws protecting such data.

What is private data?

There has been a great deal of discussion as to what private information is and what it is not. The Federal Trade Commission (FTC) distinguishes data as being either "public" or "non-public" personal data. Public data is considered to be anything that is "reasonably" believed to be publicly available (e.g., telephone numbers listed in a directory). Non-public personal data is defined as data that is "personally identifiable financial information" (c.f. https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm). An example of this may be information such as Social Security Number, income, etc. that may be given while applying for loan.

However, not all data needs to be financial to be considered private. With online availability of a variety of information (e.g., health records), the definition of private data is continually evolving. Under Section 1171 (Part C of Subtitle F), health information includes anything oral or recorded that is received by the health care provider which relates to the past, present or future of any individual. Because so much data is now stored/available online, a succinct definition is difficult and has caused issues concerning what is or isn't private data.

For example, in 2016, legislation was passed that required ISPs to get permission from customers (or have them opt-in) whereas before the ISP could sell their data and browsing history (Coldewey, 2016). Less than a year later, new legislation repealed the law, going back to the system where customers are required to explicitly request for their information to remain private (Hatmaker, 2017). Thus, the overruling of the "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services Act" has demonstrated that the idea of "private data" is continually changing and there are differing views of private data from an ISP's perspective compared to a consumer idea of private data.

For the current discussion, private data will be defined as personal data the individual does not want to make available to the public. This includes things such as passwords, financial records, personally identifiable records (e.g., social security number).

Federal Laws

Currently, the primary information security law that has provided guidelines for subsequent law s is the *Federal Information Security Management Act of 2002* or FISMA (US Congress, 2002a). While this legislation does not apply directly to the private sector, and instead mandates a certain type of behavior from the public sector, it is an important foundational piece of legislation which has helped to inform subsequent policy and can be used to justify security practices in the private sector. FISMA, "requires the Director to establish and operate a central Federal information security incident center; and head of each agency operating or controlling a national security system to take measures to protect such system." This legislation mandates the creation and operation of an information security incident center. This requirement is helpful in providing a

precedent for other organizations to follow, noting that creating a place for managing security incidents and protecting systems that possess sensitive information is a followed practice by the US government.

FISMA also states that standards will be issued by the National Institute of Standards and Technology (NIST), and that each Director, must assist in promulgating standards. The implicit rationale with mandating that the National Institute of Standards and Technology oversee developing and submitting guidelines, is that experts who are well informed regarding the most current threats can continually update and redefine standards. More will be discussed on the importance of NIST in the discussion section.

While having a bill that mandates all departments in the US Government comply with a set information security standards, creating legislation that accomplishes the same goal for all sections of the private sector has proven to be a challenge. Because of the variety of data collected and stored by different industries and companies, much of the regulation within the private sector has been industry specific. The following are a few of the industry specific laws currently in place:

- **Sarbanes-Oxley Act of 2002 (SOA)**
  This act dictates that companies who handle financial records must retain them for at least seven years (US Congress, 2002b). This act applies to accounting firms, and any type of organization the manages financial records. SOA has been amended several times since its passage into a law to bolster penalties for companies who have been failing to comply with regulations. The Public Company Accounting Oversight Board (PCAOB) is charged with overseeing, regulating and disciplining.

- **Health Insurance Portability and Accountability Act of 1996 (HIPPA)**
  This act applies to any and all offices which handle data related to healthcare of patients and, in an effort to simplify healthcare, shifts information to electronic form while protecting a patient's personal health information (US Congress, 1996). This legislation has very clear standards regarding who should be able to have access to patient data, and how this data should be stored and managed. Health and Human Service's Office of Civil Rights is charged with enforcing these regulations.
- **Gramm-Leach-Bliley Act**
  This act dictates that financial institutions are required to protect private information of clients and customers. The Federal Trade Commission (FTC) currently helps to enforce this act (US Congress, 1999).

- **Family Educational Rights and Privacy Act of 2011 (FERPA)**
  This act applies to a student's records and the rights of parents to see (or not see) performance and other evaluative data. This act applies to those schools receiving federal funding for any program. It does have an exemption for the types of data that might be seen by parents of a minor.

These laws are some of the most commonly referenced legislation that applies to the private and potentially public sector and relates to information security. However, this does not cover many of the issues commonly associated with security breaches and privacy issues. This evokes the question: Do the laws that we currently have in place protect consumer data and information? This is often left to individual states which will be discussed next.

State Laws

In addition to the federal restrictions that are in place, companies must also be aware of local (i.e., state) laws that mandate specific types of security protocol or procedure for managing sensitive data, or reporting compromises of that data. Much of the legislation concerning privacy and security of individual data has been placed at the state instead of the federal level. Because of this, it is common for new cybersecurity legislation to be introduced yearly at the state levels to keep up with the ever-changing cybersecurity landscape.

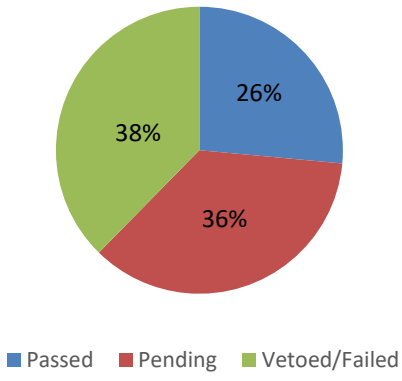

Figure 1. 2015-16 State Security Legislation Introduced and Status

For example, per the National Conference on State Legislatures (www.ncsl.org), over 170 new cybersecurity laws have been introduced across 37 states in the past 2 years (2015-2016). Figure 1 shows how many of these have passed, are pending votes or have been vetoed/failed. The data reflects that while 38% have failed to receive legislative approval, over 60% are still in the consideration stage. This shows the ever-evolving landscape of legislation that organizations must address.

The most active states in this arena are New York, California and Washington. Surprisingly, Delaware which has a significant number of corporations registered only had 2 laws pertaining to privacy and security
At the state level, laws concerning security and privacy include security breach notifications, data disposal and identity theft protection. While there are other laws that vary state to state, these laws and regulations are specifically focused on individual data and are common in most states. These laws will be discussed further in the following subsections.

Security Breach Laws
Currently, 48 states as well as Puerto Rico and the District of Columbia have passed laws requiring both private and government agencies to notify individuals when breaches occur. These will typically include: who should be informed, a definition of what private data is, what constitutes a breach, etc. The first such law was enacted by the state of California in 2002.

California State Bill 1386 states that:

> "Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person (California State Senate, 2002, Section 1798.82 a)."

As this law set the basis for most other state breach laws, it is important to point out that it specifically relates to businesses that conduct business in California and the distinction of California residents. Thus, in states such as Alabama and South Dakota which lack such laws, there is no legal obligation to notify residents of security breaches. The challenge for organizations is that with 48 states writing their own privacy and security laws there are many varying requirements.

Data Disposal Laws
As of the end of 2016, 31 states and Puerto Rico have enacted laws pertaining to: "the destruction, disposition or otherwise make personal information unreadable or undecipherable". (National Conference of State Legislature (NCSL)). The FTC (Federal Trade Commission) has also enacted legislation requiring the proper disposal of individuals' information.

Interestingly, of the states that have passed data disposal laws, all the laws apply to businesses within their state, but only 13 of 31 apply to state and local governments. Following is an example from the state of Delaware on what must be destroyed to make these data elements non-readable:

> "Personal identifying information'' means a consumer's first name or first initial and last name in combination with any 1 of the following data elements that relate to the consumer, when either the name or the data elements are not encrypted: Social Security number; passport number; driver's license or state identification card number; insurance policy number; financial services account number; bank account number; credit card number; debit card number; tax or payroll information or confidential health-care information including all information relating to a patient's health-care history; diagnosis condition, treatment; or evaluation obtained from a health-care provider who has treated the patient which explicitly or by implication identifies a particular patient.(State of Delaware, Title 6, Commerce and Trade, Chapter 50, 2014)."

In the area of data disposal, the federal government through the FTC and the Graham Leach Bliley Act tend to provide significant guidance as most states have deferred to the FTC guidelines in the area of financial records. The FTC defines proper disposal as:

> "Practices that are reasonable and appropriate to prevent the unauthorized access to – or use of – information in a consumer report. For example, reasonable measures for disposing of consumer report information could include establishing and complying with policies to: burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed; destroy or erase electronic files or media

> containing consumer report information so that the information cannot be read or reconstructed; conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule (Federal Trade Commission, 2017)."

In summary, the data disposal laws provide clearer guidelines than other areas of data privacy as the records are more tangible in either electronic or written form.

Identity Theft Protection Laws

In just the past two years, federal legislation was written to future enhance Identity Theft (Department of Justice, 2017). This legislation defines identity theft as knowingly using another individual's identifying information for illegal purposes. At the state level, all 50 states have passed some form of identity theft laws, with the penalty ranging from felonies in Alabama to just misdemeanors in Virginia. NCSL, 2017).

Several states have enacted more stringent legislation. An example is the North Carolina "Identity Theft Protection Act," which describes the consumer's rights to their data and information, allowing them to effectively 'freeze' companies out of obtaining copies of the individual's credit report. The legislation also mandates that companies take "reasonable measures to protect against unauthorized access to or use of…" sensitive data, and requires businesses to report security breaches if any consumer data has been compromised. Per the North Carolina Department of Justice, 3,400 breaches have been reported, which have affected 9.3 million North Carolina consumers. While potentially burdensome to monitor this information, it is clear that requiring companies to report breaches is an important part of the legal infrastructure around information security. If breaches in security did not mandate a report, millions of consumers could be at risk to damaged credit, identity theft, and other forms of crime. The state of North Carolina has prioritized the importance of their citizens to be protected, and informed when they need to make changes in order to remain safe. (North Carolina, 2005).

Legislatures also face the dueling priorities of increased data privacy and protection versus the costs to businesses. A recently introduced bill mandates a report which reflects the cost of, "(1) security for computers, networks, software, storage systems, data transmission, equipment, and support services; (2) measures to mitigate and hedge against compromises of information systems; and (3) economic loss or harm caused by such compromises." The findings in such a report could lead to some sweeping improvements in upcoming bills. Reporting on the cost of security measures versus the cost of security breaches and how that directly effects the economy could produce updated legislation that focuses on flexible and agile methods for mandating security. This would provide companies with requirements for protecting consumer data, while allowing them to do so in a way that was cost effective and could easily be updated or modified to adjust to new, yet unknown, threats.

3. DISCUSSION OF FUTURE CYBERSECURITY LEGISLATION

Security and privacy legislation continues to evolve at both the state and federal level. As previously mentioned, laws at the federal level focus on specific industries while state laws attempt to focus on individuals within those states. The following section discusses the current issues with legislation and potential direction the US should follow moving forward.

Private Data

One issue present in both federal and state laws is the definition of what is and what is not private. Federal laws are based on the industry they regulate thus much of the definition of private data is industry specific (e.g., HIPPA focusing on health information). However, while many state laws are similar, there is no requirement to be consistent across states when it comes to the definition of private data at the state level. We recommend that this is something that should be addressed at the federal level to provide a constant definition regardless of residency. However, this may be a moot point as recent surveys have shown that many of the employees working with private data may not know the laws in place.

While there is an argument over what type of personal data should be protected, or considered private, a new survey conducted by Dell, shows that even if legislation requires groups and companies to adhere to strict guidelines regarding sensitive information, it may not be enough. The survey resulted in having 72 percent of professionals stating that they would be willing to share sensitive, confidential or regulated information (Dell Technologies, 2017). This type of overwhelming response is frightening in its implications, leading us to believe that regulations and compliance policy for protecting

information and data are relatively useless in the face of disregard for said policies.

While the reports of the study go on to explain some of the circumstances in which employees might have felt it was acceptable to share data, companies should be taking more responsibility for explaining the importance of maintaining proper security practices when it comes to sensitive information. Thus, not only should there be a definition of private data at the federal level, there must also be a change in how organizations inform their employees of such laws and regulations relation to privacy and security.

Federal or State?

The broader concern for security and privacy laws lies in where these laws exist – the federal level or state level. Currently, federal laws are enforced across a broad range of agencies including the Federal Trade Commission (FTC), Health & Human Services and the Public Company Accounting Oversight Board. In 2016, under the Obama administration, the Cybersecurity National Action Plan was implemented to help move the US enhance cybersecurity awareness and protections (Daniel, et al., 2016). While much of the plan focused on the federal level, it also had actions to enable individuals to increase security (e.g., requiring multi-factor authentication) to protect their identity online. However, while the action plan was a step forward, it was only an action plan with no specific legislation tied to it. We recommend that future 'state' laws cease to exempt themselves from the privacy laws and impose restrictions upon state and local government for compliance.

Recently, the new administration has issued an Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (Gottlieb, 2017). This requires federal agencies to adopt of the Framework for Improving Critical Infrastructure Cybersecurity developed by NIST. While this is an important step forward for federal agencies, the order does not require any private agencies to follow such guidelines. This is where the federal agencies can be proactive by requiring the implementation of NIST guidelines in organization across the US to increase the security of the infrastructure which in turn reduces the need of breach notification laws.

What should occur at the state level? This is a question that has stirred much debate in the cybersecurity industry. Some states have been much more proactive than others. California and New York lead with more developed and stringent security laws. For example, New York recently enacted legislation requiring financial firms to go beyond compliance of Gramm-Leach-Bliley Act (Reuters, 2017). These regulations include increased scrutinization of third-party vendor security, risk assessments to design programs specific to the firm and an annual certification of compliance. While this covers firms in New York, what happens to those operating in Chicago or Boston? It is evident that the focus on standardization at the federal level must also be implemented at a state level as well. An example of the exposure to third party vendor liability was the 2014 theft of consumer accounts at Target Stores. The theft occurred via the network of a heating and air vendor.

Nature of Cybersecurity

One of the most important questions is whether complying corresponds to more secure information. The goal of creating regulation to protect information and sensitive data is for that data to be secure and private. However, Black (2017) suggests there is a clear defect in regulation as it lags far behind the innovation of those trying to get to the data (i.e., hackers or the 'bad guys'). He argues that current iterations of cyber and information security policy are outdated compared to the current threats especially as companies focus on compliance with a law that was designed to protect against threats that are several iterations older than its current form. The article proports that the expense of coming into compliance is so heavy that companies are dissuaded from pursing real security measures, which seem to add more cost, without providing any legal incentive. As noted earlier legislatures are incorporating consideration of the costs of implementation versus potential loss of data into their future laws.

The author claims that providing legislation that requires companies to protect consumer data and not to disclose it without approval and having the legislation remain open ended regarding the implementation of any security measures used in order to maintain security over the consumer's private data is the best method for providing actual compliance, and allowing for companies to continue to grow flexibly and expand their security measures in an elastic way (Black). This theory, however, assumes that the company has tech experts who are able to implement flexible, high level, agile systems. Unfortunately, there are many businesses without the means to do so. By ridding legislation of any details in how to get into compliance, information security becomes a much larger hurdle for companies who are not steeped in information security systems.

Business' Perspective

While security and privacy laws are in place to protect the individual, companies must also shoulder the burden of these laws, often at a cost to the organization. Even within larger companies, executives like CIOs, Security Officers and other experts are often expected to know which laws apply their respective industry and how to apply the requirements to their prospective programs, however that does not always happen to be true (Burke 2003). While the details on compliance are stated in the laws themselves, the challenge is finding the full laws and knowing which ones are required to be compliant. This becomes more difficult for small companies who wish to work as contractors for the government, an odd place where the public and private sector meet and in addition to your local and federal legislation you must also consider FISMA. This can be so overwhelming as to detract companies who could provide services to the government from pursuing that option, it can also scare people away from creating new businesses in general.

Beyond understanding which regulations are applicable, the burden of becoming compliant are substantial for both small and large companies, as your companies grow so does the required scale of your security apparatuses. For smaller companies the financial expense can be business-squashing. Being able to afford an expert in security will be out of reach for many small businesses, and hiring a third-party company is a large upfront cost for a company who is just getting started. Because of these costs, it is likely that many startups either forego security compliance, or fail to invest in the company's growth potential. A bright spot for smaller firms will be the moving of their data centers to cloud service providers that will be able to provide increased security not feasible for smaller firms. Larger companies often face the same choices, as updating security systems becomes so overwhelming that they either update too slowly, or potentially stagnate due to inability to handle more growth based on their current systems (Vanderburg, 2011).

4. CONCLUSION / RECOMMENDATIONS

The question of protection of an individual's security and privacy of data is not easily answered. The landscape for both individuals and organizations is vast and often challenging to understand. Ultimately, it may come down to the federal government to lead the race to security and privacy regulations for securing systems. However, these regulations are also in desperate need of revamping.

Much of the current federal legislation was originally drafted in the 90s or early 2000s, fifteen to twenty-five years later the requirements for maintaining up to date security measures look very different. The rate at which threats that exist to information security are evolving continue to grow at a steady clip. While regulations can be burdensome to companies, ridding the government of the responsibility to hold institutions accountable for maintain privacy for citizen's private data would be unconscionable. Instead, amending legislation in an effort to produce a more flexible system for maintaining compliance with regulations would be a welcome shift to the current processes that are in place. Having updated standards of security results used as a measurement of compliance, as opposed to having detailed methods of hardware and network setup would be much more effective, particularly for larger companies, or companies with onsite technology experts with the capacity for implementing a proper security system.

State legislatures also need to be involved as they tend to enact more legislation in this area. It is imperative that security associations work with state representatives to provide them the expertise to enact meaningful legislation at the state and local area.

This does not necessarily solve the problem for smaller companies, who may not have access to experts, or the funding to hire them. A possible solution to this problem would be to have a certification program for hardware that falls into compliance with the current security standards, and to make this list of certified hardware available to the private sector. Part of the certification condition would be that the hardware must be updated on a consistent basis, to provide security updates to all businesses who purchased the hardware in an effort for that company's hardware to remain compliant. This would rid small businesses of the need to have on site experts, and they could instead focus the time and energy on growing their company. In addition to requiring certain hardware parameters, companies should be required to hold more training sessions, or produce some sort of reporting showing that their employee base is staying up to date with proper information security handling procedures.

Employees should be required, by law, if handling sensitive information, to either obtain some type of certification as evidence of their competence in information handling, or the employer should be

able to produce some type of proof of their training system and employee retention of relevant material.

While the perfect ratio of regulation to innovation in the realm of information security remains obscured, the perpetual buzz of threats, viruses, and exposed information continues to become a louder noise in the zeitgeist. As the conversation continues to grow, in addition to providing more context for businesses to take information security seriously, it should also allow for consumers to become more educated about where they choose to spend their money and share their personal information with.

If a company is known to sell information, or handle sensitive data sloppily, consumers should become more aware and choose not to associate with that organization. Although regulations may produce added cost to companies, they also provide a level of protection and resource for consumers, an important aspect that society is still struggling to understand.

5. REFERENCES

Black, D. (2017, May 2). Security Regulations vs. Cybersecurity: the War. White Paper. Coralville: SANS Institute InfoSec Reading Room. Retrieved May 3 2017 from http://www.huffingtonpost.com/entry/security-regulations-vs-cyber-security-the-war_us_59089d7ce4b03b105b44bc22

Burke, T. (2003). U.S. Government IT Security Laws. SANS Institute InfoSec Reading Room. Retrieved April 30 2017 from https://www.sans.org/reading-room/whitepapers/legal/us-government-security-laws-1306

California State Senate (2002). California State Bill 1386, Personal Information: privacy. Sacramento, CA.

Coldewey, D. (2016, October 27). New FCC rule protects users from the prying eyes of ISPs. Retrieved May 24, 2017 from https://techcrunch.com/2016/10/27/new-fcc-rule-protects-users-from-the-prying-eyes-of-isps/

Daniel, M., Scott, T. and Felten, E. (2016). The President's National Cybersecurity Plan: What You Need to Know. The White House Blog. Retrieved June 6, 2017 from https://obamawhitehouse.archives.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know

Dell Technologies (2017). Dell End User Survey 2017. Retrieved May 24, 2017 from http://dellsecurity.dell.com/wp-content/uploads/2017/04/2017-Dell-End-User-Security-Survey_FINAL.pdf

Department of Justice (2017). Identify Theft: What are Identify Theft and Identity Fraud?. Last Retrieved June 7, 2017 from https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Federal Trade Commission (2017). Disposing of Consumer Report Information. Retrieved June 5, 2017 from https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how

Financial Services Committee (2002). *Sarbanes-Oxley Act of 2002*: United States Congress.

Gottlieb, R. (2017, May 25). President's Executive Order on Cybersecurity: Impact on Banks Unclear. Retrieved June 2, 2017 from http://www.lexology.com/library/detail.aspx?g=c02d0271-d879-493d-a5ec-ff3b85ee7bf4

Hatmaker, T. (2017, March 28). Congress just voted to let internet providers sell your browsing history. Retrieved May 24, 2017 from https://techcrunch.com/2017/03/28/house-vote-sj-34-isp-regulations-fcc/

National Conference of State Legislatures (2017). Data Disposal Laws. Retrieved June 1, 2017 from http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx

NCSL (2017). Identity Theft. Retrieved 6/6/2017. https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Nieles, M., Dempsey, K., and Yan Pilliteri, V. (2017). An Introduction to Information Security. National Institute of Standards and Technology. Retrieved June 7, 2017 from http://csrc.nist.gov/publications/drafts/800-12r1/sp800_12_r1_draft.pdf

North Carolina (2005) Chapter 75 Article 2A. Identity Theft Protection Act. 2005. Bill. Retrieved June 7, 2017 from http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/ByArticle/Chapter_75/Article_2A.html

Reuters. (2017, February 16). Here's When New York State's Cybersecurity Rules Take Effect. *Fortune*.com. Retrieved May 15, 2017 from http://fortune.com/2017/02/16/newyorkstatecybersecurityregulation/

Sherr, I. (2017). WannaCry ransomware: Everything you need to know. Retrieved May 23, 2017 from https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/

State of Delaware (2016). Safe Destruction of Records Containing Personal Identifying information. Retrieved June 5, 2017 from http://delcode.delaware.gov/title6/c050c/index.shtml

Vanderburg, E. (2011). Information Security Compliance: Which regulations relate to me? Retrieved April 30, 2017 from http://www.jurinnov.com/information-security-compliance-which-regulations/

Washington Post (2017), "What to expect now that Internet Providers can collect and sell your browser history, Retrieved 6/5/2017, https://www.washingtonpost.com/news/the-switch/wp/2017/03/29/what-to-expect-now-that-internet-providers-can-collect-and-sell-your-web-browser-history/?utm_term=.437383d9f7d3

US Congress (1996). Health Insurance Portability and Accountability Act of 1996. Washington, DC.

US Congress (1999). Gramm-Leach-Bliley Act. Washington, DC.

US Congress (2002a). Federal Information Security Management Act of 2002. Washington, DC.

US Congress (2002b). Sarbanes-Oxley Act of 2002. Washington, DC