



University of Kentucky  
**UKnowledge**

---

Theses and Dissertations--Communication

Communication

---

2016

## Protecting Online Privacy

Stephanie D. Winkler

University of Kentucky, [sdwinkler1@gmail.com](mailto:sdwinkler1@gmail.com)

Digital Object Identifier: <http://dx.doi.org/10.13023/ETD.2016.130>

[Right click to open a feedback form in a new tab to let us know how this document benefits you.](#)

---

### Recommended Citation

Winkler, Stephanie D., "Protecting Online Privacy" (2016). *Theses and Dissertations--Communication*. 47.  
[https://uknowledge.uky.edu/comm\\_etds/47](https://uknowledge.uky.edu/comm_etds/47)

This Master's Thesis is brought to you for free and open access by the Communication at UKnowledge. It has been accepted for inclusion in Theses and Dissertations--Communication by an authorized administrator of UKnowledge. For more information, please contact [UKnowledge@lsv.uky.edu](mailto:UKnowledge@lsv.uky.edu).

## **STUDENT AGREEMENT:**

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

## **REVIEW, APPROVAL AND ACCEPTANCE**

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Stephanie D. Winkler, Student

Dr. Sherali Zeadally, Major Professor

Dr. Bobi Ivanov, Director of Graduate Studies

PROTECTING ONLINE PRIVACY

---

THESIS

---

A thesis submitted in partial fulfillment of the requirements  
for the degree of Master of Arts in the College of  
Communication at the University of Kentucky

BY

Stephanie Winkler

Lexington; Kentucky

Co-Directors: Dr. Sherali Zeadally Professor of Communication

and Dr. Bobi Ivanov, Professor of Communication

Lexington, Kentucky

2016

Copyright © Stephanie Winkler 2016

## ABSTRACT OF THESIS

### PROTECTING ONLINE PRIVACY

Online privacy has become one of the greatest concerns in the United States today. There are currently multiple stakeholders with interests in online privacy including the public, industry, and the United States government. This study examines the issues surrounding the protection of online privacy. Privacy laws in the United States are currently outdated and do little to protect online privacy. These laws are unlikely to be changed as both the government and industry have interests in keeping these privacy laws lax. To bridge the gap between the desired level of online privacy and what is provided legally users may turn to technological solutions.

**KEYWORDS:** Online Privacy, Privacy Laws, Technology, Encryption,  
United States

---

Stephanie Winkler

---

4/25/16

---

PROTECTING ONLINE PRIVACY

BY

Stephanie Winkler

Dr. Sherali Zeadally

---

Director of Thesis

Dr. Bobi Ivanov

---

Director of Graduate Studies

4/25/16

---

## ACKNOWLEDGMENTS

This thesis, while completed individually, would not be what it is today without the guidance of several individuals. First and foremost, I would like to thank my chair Dr. Sherali Zeadally whose example has been instrumental to this thesis and my development as a scholar. In addition, Dr. Anthony Limperos was always available for helpful criticism and insight during the entire thesis process. I would like to thank Dr. Bobi Ivanov for extending his support for me to move forward with this thesis. Finally, I would like to thank my entire thesis committee Dr. Sherali Zeadally, Dr. Anthony Limperos, and Dr. Michail Tsikerdekis for devoting time out of their busy schedules to help with the preparation of this thesis and the defense.

## TABLE OF CONTENTS

List of Figures.....	v
Chapter One: Introduction	
Background .....	1
Communication Privacy Management.....	2
Research Questions.....	6
Methods.....	7
Chapter Two: United States Privacy Laws	
Introduction.....	7
United States Privacy Laws.....	8
Summary.....	18
Organization Policies.....	23
Policy Recommendations.....	25
Chapter Three: Barriers to Privacy Protections	
Introduction.....	28
Industry Objections.....	28
Law Enforcement Objections.....	30
Summary.....	32
Chapter Four: Privacy Enhancing Technologies	
Introduction.....	32
Data Collection Methods.....	33
Types of Data.....	34
Privacy Enhancing Technologies.....	35
Anonymity Technology.....	48
Chapter Five: Discussion and Conclusion	
Summary.....	51
Limitations and Future Research.....	53
Conclusion.....	54
References.....	56
Vita.....	65

## LIST OF FIGURES

Figure 1, Ghostery Sign-up Screen.....	36
Figure 2, Disconnect Interface.....	38
Figure 3, Privacy Badger Interface.....	39
Figure 4, Off The Record Plug-in Button in Pidgin.....	45
Figure 5, Off The Record Plug-in Drop Down Menu.....	46
Figure 6, Dmail Function within Gmail.....	47
Figure 7, Privnote Online Form.....	48
Figure 8, TOR Browser Menu.....	50
Figure 9, TOR Privacy and Security Setting Levels.....	51



## Protecting Online Privacy

The Internet has grown in importance in the United States with 87% of adults reporting that they used the Internet in 2013 (Pew Research Center, 2014). This is a significant increase from the 14% of adults that reported using the Internet in 1995 which was only a few years after the Internet was first introduced commercially (Pew Research Center, 2014). The widespread use of the Internet has played an integral part in shaping the United States today by breaking down communication barriers and opening doors for the average person to be a content creator. These changes have sparked public debates about rights and regulations in a digital age. At the center of these debates is the nature of what is considered public, and what is considered to be private.

The line between public and private has become blurred online (Barnes, 2006; Strauß & Nentwich, 2013). Information that is typically only shared with specific people in an offline setting is widely available to others online (Albanesius, 2010). This phenomenon is even more pronounced when examining social platforms which are based around sharing personal information online (Chen & Michael, 2012). With social media currently being used by 70% of all Internet users (Duggen et al., 2015), people are moving more of their lives online. Despite the tendency to publically post information in places easily accessible (like social media), users express feelings of their privacy being violated when the information is accessed by an unintended audience (Barnes, 2006).

Online privacy has been a popular topic in academic research for over a decade.

However, the concept of online privacy was pushed into popular media after Edward Snowden leaked classified National Security Agency documents in 2013 (Preibusch, 2015). After the Snowden revelations most Americans believe that their privacy is being

threatened (Madden, 2014) with 66% of adults stating that the current laws are not enough to protect online privacy (Rainie, Kiesler, Kang, & Madden, 2013). Though this feeling is prevalent there is little research into how online privacy is protected in the United States. This study seeks to explore the online privacy protections available to users.

## **1.1 Online Privacy**

Even though there is an expressed concern for online privacy in both popular culture and research, online privacy does not have a consistent definition. This is partly because privacy is a difficult term to define since the term itself is highly subjective. Since one of the ways that privacy definitions vary is by culture our definition of privacy will be limited to the United States. Privacy must be conceptualized in the context of online activity since there are significant differences between the offline and online worlds. Many offline activities can be conducted without any observation of others which means privacy can be conceptualized in terms of secrecy (Kemp & Moore, 2007). However, any activity online leaves behind a trail of information also known as a digital footprint (Weaver & Gahegan, 2007). A digital footprint can be composed of numerous types of information including metadata (e.g. location, Internet Protocol address), search history, email, and social media posts (Steve, 2013). A user's digital footprint is what the majority of online privacy research is concerned about either in part or in whole (Moore, 2012). The most common definition of online privacy is derived from this idea of a user owning and managing their digital footprint. This conceptualization of online privacy examines privacy as a form of control. This means that the more control the user has over their digital footprint; the more privacy they have (Kemp & Moore, 2007; Moore,

2008). However, the concept of online privacy is more complex than just being a form of control over a digital footprint. This definition leaves out phenomena that has been observed by researchers on social networking sites. Users of social networking sites do not always feel that their privacy has been violated when information is posted about them to the site (Levin & Abril, 2009). If the definition of privacy as control over information was completely accepted, this circumstance should result in a privacy violation from users since they have no control over the information being posted. However, users do express a privacy violation when information is shared outside of their social network (Levin & Abril, 2009). The theory of communication privacy management can explain this part of online privacy.

## **1.2 Communication Privacy Management**

Communication privacy management (CPM) provides a framework for understanding how people create and maintain privacy boundaries. This theory is based on the core concept that people see themselves as owners of their private information (Petronio, 2010). Because they own this information they feel that they have a right to control this information. This fits neatly with how laws, organizations, and researchers see online privacy as a form of control. When this control is lost in some way, like being shared without consent, they feel as if their privacy has been violated (Petronio, 2010). This concept is demonstrated online when online platforms share their user's information with a third party. If the user did not feel that they gave permission for their information to be used that way, they expressed that their privacy had been violated (Rainie & Duggen, 2016).

When an owner of private information discloses that information to third party, the third party then becomes a co-owner of that information. All owners of the private information have a degree of control over the information. How much control an owner has is negotiated depending on the situation and the information (Petronio, 2010). This negotiation process can vary greatly. For instance, privacy negotiation can be explicit (“don’t tell anyone”) or implied (taking someone aside to tell them/sending a private message) (Kennedy-Lightsey et al., 2012). The rules resulting from the negotiation detail how, with, and who the information can be shared. When someone breaks these rules either intentionally or unintentionally, boundary turbulence results (Kennedy-Lightsey et al., 2012; Petronio, 2010). In the situation with the online platform and the user, the user disclosed some information to the online platform for the platform to use. When the platform disclosed this information to a third party it violated the privacy rules from the view of the user since they did not give consent for the third party to use the information. After the privacy violation the user experiences boundary turbulence, which in this case manifests itself as distrust in the online platform (Rainie & Duggen, 2016). However, in order for this boundary turbulence to occur, the user has to realize that there was a privacy violation to begin with. This turbulence tends to manifest when the user experiences either problems with a security breach, or sees evidence that their behavior is being tracked.

While this theory was developed to describe privacy negotiations in interpersonal relationships, the main principles are still applicable to online privacy since it focuses not on the private information itself, but the management of the information. Since the development of the theory in 1991 it has been applied in many areas including family

communication, health information disclosures, online social networks, and blogs (Petronio, 2013). However, the area that is most relevant to online privacy is the use of the theory in online social networks. CPM can explain the previous example of private information shared on a social networking site. In order to avoid confusion, the two users will be referred to as Alice and Ben. Alice and Ben both belong to the same social network and are friends with each other. In this situation Alice shares what is considered private information about Ben to their group of friends online. Alice did not ask Ben if she could share this information, yet Ben does not feel there was a privacy violation. In this situation the rules negotiated by Alice and Ben were not violated with this disclosure. Opponents to privacy as a form of control state that this same situation would be different if the information was different (Levin & Abril, 2009). CPM explains this change by saying that the rules regarding the disclosure of the information has changed. So, while online privacy is the user having control over one's information the amount of control can change depending on the given situation.

When looking at online privacy through the lens of CPM the nature of the debate changes. This exposes the underlying problem with online privacy to be one of boundary rule violations. Boundary rule violations can occur in a wide variety of circumstances either intentionally or unintentionally. An unintentional violation can be as simple as an accidental slip, disclosing the information without realizing that's what happened, but can also occur because of some form of miscommunication between the co-owners of the information (Petronio, 2004). If the rules were not identified explicitly in the negotiation or not understood by either party, unintentional boundary violations are likely to result. Boundary rule negotiations do not occur very often online when it is between a large

organization and the end user. When these negotiations do occur it is typically in the form of a privacy agreement that the user most likely has not read (Malaga, 2014). However, there is no consent form when a user opens their web browser or any discussion with larger institutions about how their information should be treated. In this situation without boundary negotiations, many users feel that another party has acted in behalf of them. At this time, many users believe that different activities online are protected by law as private (Peralta, 2013). This belief may not be consistent with the current laws and all online activities may not be treated equally. This leads to the first research question

***R1: What are the laws currently in place (if any) to protect a user's online privacy?***

Over the years, activities online have become progressively more public. Part of this is related to online social networks and the blurring of the line between public and private (Vitak, 2012). Not surprisingly, people have started to become aware that they have little expectations of privacy online and are calling out for more privacy protections (Risen, 2015). Only this year (2016) was the Electronic Communications Act of 1986 revisited (Kelly, 2016) in light of new technology, even when advocates have long stated that the language is outdated (Sidbury, 2001). This leads us to the second research question

***R2: What are the potential barriers to greater online privacy protections?***

The answers to these questions still do not offer much to the user in terms of privacy management when they are not a party to the boundary negotiations. This leads us to our final research question

***R3: What measures are available for users to have greater online privacy protection?***

These research questions will be addressed by looking at the current privacy laws in the United States at both a federal and state level. In addition, the rules currently governing the institutions involved with user privacy agreements will be examined. Research question 2 will be addressed by examining the state of technology today, online platform business models, and potential governmental interests in the state of online privacy. Research question 3 will be answered by detailing a list of methods that users can employ to protect their own privacy when institutions fail to protect their privacy rights. These methodologies include both technical and social solutions to protecting online privacy.

## **2. Privacy Laws Today**

The United States has an interesting approach to protecting online privacy compared to other major world powers. There is not a dedicated governing body for privacy issues and not a single comprehensive privacy law. Instead, there are many different privacy laws each covering a small subsection of privacy. This results in a patchwork design where many pieces of cloth are sewed together to make a whole, but not all of the pieces fit together perfectly and there are a few holes here and there (Soto & Simpson, 2014).

There are an estimated 14 United States laws that have measures to protect online privacy. This list primarily covers the United States federal laws. There are numerous state laws that strengthen online privacy protections in the United States, but currently there is no known method of comprehensively reviewing state laws across all 50 states. The majority of these laws were passed before the start of the 21<sup>st</sup> century and many of them have no mention of the Internet. Instead, it is assumed that the protections provided

to offline services extend to online as well since they were implemented to protect the data itself. These protections should not change regardless of what form the data is in or where it is stored. The privacy protections in these 14 laws are summarized as followed:

## **2.1 Summary of Privacy Laws**

### **Cable Communications Policy Act of 1984**

The Cable Communications Act was enacted in 1984 and applies to cable companies and service providers. This act contains provisions regarding information security, data collection and data access. The information covered under this law known as personal identifiable information (PII), which is any information that can be used to identify a particular user. The privacy protections specified in this law do not apply to aggregate data. All cable companies and service providers must have a privacy policy that specifies the nature in which PII is used, collected, and duration of time it is saved. The company can only use the cable system to collection information when the information is deemed necessary to provide services or detect the unauthorized use of services. This information cannot be collected or disclosed without the user's content. The company is permitted to disclose information without the user's consent if it is necessary to conduct business, to a court, or if the disclosure is only a list of names and addresses. Subscriber's do have the right to access the information collected from them and take civil action if the law is violated by the company.

### **California Online Privacy Protection Act of 2003**

The California Online Privacy Protection Act of 2003 requires that all web platforms that engage in online data collection must conspicuously post their privacy policy on the



website. This law covers third parties that the web platform might share information with. The privacy policy must state how the user can make changes to their information, how find changes to the privacy policy, and identify the type of information that the website collects. An amendment to the law in 2013 requires web sites to also post how they respond to “Do Not Track” signatures or other methods consumers use to indicate they do not wish for persistent identifiers to be used to track their online behavior.

#### California Security Breach Information Act

The California Security Breach Information Act requires any state, person, business, or other agency that has computerized personal information data to disclose any security breach that would expose unencrypted information of California residents to unauthorized persons. Personal information data is defined as data that includes the first and last name of the individual when combined with either their social security number, driver’s license number, bank account number, or credit card number when the information is not encrypted. Personal information does not include anything that is in publically available records. Entities can provide notice of security breaches by notification of statewide media, posting the breach on the agency’s website, email, or written notice.

#### Children’s Online Privacy Act of 1998

The Children’s Online Privacy Act of 1998 (COPPA) specifies protections for children who self-identify as being under the age of 13 regarding the collection and management of information. This law applies to anyone operating a website used for commercial purpose that collects and maintains personal information. This law also applies to any

third parties and advertisers that have content on the site and know that they are collecting information from children. Personal information includes the child's first and last name; home or physical address; email address; phone number; social security number; and any other identifier that permits contact. Personal information could also include information concerning the parents of the child when combined with one piece of the child's personal information. In 2013 the law was updated to include geolocation data and persistent identifiers in the definition of personal information. These entities must provide notice to the parents of what information is collected from the child, how the information is used and information sharing practices. Parents must give consent for the collection, use, and disclosure of their child's information. The parents also have the right to receive information regarding the type of information collected and the information that is collected from their child. Permission for the entity to use or maintain the information can be refused, however, the entity has the right to terminate the service if the parents refuse to allow the information to be used.

There are a few exceptions where the parents do not have to give consent for the entity to use the child's information. These circumstances include when contact information is used to respond once to a child and not used to contact them again; request for name or online contact information is used for the purpose of contacting the parent for consent and providing notification of collection practices; online contact information used to respond more than once to the child regarding a specific request made by the child; name and contact information if the safety of the child is in question; any situation where the information is necessary to protect the security and integrity of the site. In all of these situations the information cannot be maintained in any retrievable form.

## Communications Assistance for Law Enforcement Act of 1994

The Communications Assistance for Law Enforcement Act of 1994 criminalizes unauthorized access and disclosure of information in electronic storage. Specifically, it is illegal to gain access without authorization or exceed an authorization to access a facility which provides electronic communication and prevent access, alter, or obtain electronic communication while it is in storage. The law does not apply to conduct authorized by the entity providing the electronic service or user of said service. The entity that is providing the electronic communication service to the public should not disclose the contents of any communication. In the case of providing remote computing services the entity must also not disclose the contents of communication that is carried on the service. Providers can disclose information of customers where the contents were accidentally obtained and appear to pertain to a crime or the provider can disclose information to the government if the provider has a good faith belief that an emergency relating to the death/injury of another person requires the use of the information. If the electronic communication is in the system for 180 days or less the government can require disclosure with a warrant and must give prior notice to customer. If the electronic communication is in the system for over 180 days, the government can require disclosure without the provider giving the customer notice. The records covered in this law can include first and last name; address; session times and durations; length of the service and the services used; network address; and the means or payment of services. Customer does have the right to challenge requests for information disclosure.

## Computer Fraud and Abuse Act of 1986

The Computer Fraud and Abuse Act of 1986 criminalizes a large amount of computer activities. Specifically the law criminalizes extorting money using computer based threats or threats to the computer; attempting to defraud traffic using a password or similar measure; the transmission of code or unauthorized access that damages a computer; unauthorized access or exceeding authorized access on a computer with the intent to fraud and receives something of value for the fraud; unauthorized access to government or nonprofit computers; unauthorized access or exceeding authorized access to computer and obtains financial information, information from any governmental agency, or information from any protected computer; accessing a protected computer and transmitting classified information to anyone but a United States government employee. Protected computers are defined as computers used exclusively by a financial institution or United States government agency or computers used in affecting interstate or foreign commerce or communication.

## Consumer Credit Reporting Reform Act of 1996

The Consumer Credit Reporting Reform Act of 1996 was enacted to protect the accuracy, fairness, and privacy of personal information assembled by credit reporting agencies. Credit reporting agencies are responsible for the accuracy of reports and have a duty to correct and update consumer information. The agency is prohibited from providing information that is incorrect if the consumer has given notice that the information is incorrect. Consumers have the right to view their credit file if there is an adverse action against them dependent on the information in the file. The law prohibits use of credit reports for marketing purposes and limits the use of reports to applications for credit,

rentals, and insurance; employment; court orders; business needs in transactions the customer initiated; account review; professional licensing; child support payments; and law enforcement access. If the report contains any medical information additional consent must be obtained before the information is disclosed. Individuals can take action against the agency if they are in violation of the law. The law also contains provisions to protect the security and destructions of personal information.

#### Electronic Communications Privacy Act of 1986

The Electronic Communications and Privacy Act of 1986 regulates the interception of electronic communication. Electronic communication is protected during the communication if there is no third party present, when the information is in transit, and when it is later stored. This Act prohibits the use of intercepted communications in legal proceedings without a warrant unless one or all parties consent to the recording of the communication. Private emails are protected under this act and cannot be accessed without the consent of the user. Emails that are in transit, in home computer storage, or unopened in remote storage for less than 180 days require a warrant in order to be disclosed to law enforcement agencies. If the email is opened in remote storage or unopened and stored for more than 180 days only a subpoena is required for the disclosure of the information.

#### Family Education and Rights Privacy Act

The Family Education and Rights Privacy Act details procedures regarding academic records and the rights parents have to these records. Parents and students have the right to view records maintained by the school. Educational institutions are required to have

consent from parent or student (if over 18) in order to disclose academic records. In select circumstances the institutions can disclose information without consent. Specifically, these circumstances include to school officials with an educational interest; schools a student is transferring to; officials for auditing purposes; entities a party to financial aid for the student; organizations conducting research for or on the school; in instance of a court order; when needed for emergencies relating to health and safety; and law enforcement agencies. A school can also disclose a student's name, address, phone number, email address, birthday, and dates of attendance without the consent of the student or parent. Both parents and students are required to be notified each year by the educational institution of their rights under the Family Education and Rights Privacy Act.

#### Gramm-Leach-Bliley Act of 1999

The Gramm-Leach-Bliley Act of 1999 enacted requirements for financial institutions regarding information sharing practices and safeguarding of consumer information. The institution must share details of their information sharing practices and data safeguards to the consumer and the consumer must be given notice of these policies when opening an account. This notice must explain in detail how the consumer's information is collected, shared, used, and protected. The consumer has the right to opt-out of any information sharing with parties not affiliated with the financial institution. However, the user cannot opt out of the marketing of products and/or services for the financial institution or where the information is legally required. Financial institutions are required to have a written data security plan that includes risk analysis and one employee dedicated to managing data security safeguards. In addition to this the institution must have a security program developed, maintained, monitored and tested that secures information. The institution is

responsible for changing this plan as necessary to protect the information and are strongly encouraged to have protections in place to protect against social engineering.

#### Privacy Act of 1974

The Privacy Act of 1974 establishes a code that describes how the collection, maintenance, use, and dissemination of personally identifiable information in government records is managed. Government agencies are required to give public notice about their information practices and cannot disclose any record unless they obtain written request or prior consent of the individuals of which the information pertains. Exceptions to the consent mandate include using the information for statistical purposes by the Census Bureau or Bureau of Statistics; routine use by a government agency; archival purposes; use by law enforcement; congressional investigations; or other administrative purposes. Government agencies must have both administrative and physical security systems in place to safeguard information and each agency must have a board in place that governs the integrity of data. When an information request is made the agency must state the authority under which they are asking for the information. Individuals have the right to review their records kept by the government and any amendments made to this record. The law only applies to records held by a government agency. Courts, executive components, and non-governmental agencies have no rights under this act.

#### Privacy Protection Act of 1980

The Privacy Protection Act of 1980 applies mainly to journalists and protects individuals in this field from having to turn over any work product and documentary materials, which includes sources, before the information is published. The Act prevents the search of

newsrooms specifically in order to obtain the work of journalists relating to a criminal investigation or offense. There are a few exceptions to the search provision: if the journalistic material is believed to stop the death or serious bodily harm of another human being or if the issuing of a subpoena would result in the destruction or change of documentary materials.

#### Right to Financial Privacy Act of 1978

The Right to Financial Privacy Act of 1978 extended 4<sup>th</sup> amendment protection against unreasonable search and seizure to bank records. The Act states that government agencies must provide notice and give individuals or financial institutions time to raise an objection before disclosing bank records. A financial institution is defined as any institution with the power to issue a card (debit or credit). The government may not obtain copies or access the information unless under one of the following circumstances: customer consent, court subpoena or summons, warrant, judicial subpoena, or written request from a government authority. However, if the disclosure does not identify a particular customer, is in the interest of the financial institution, in connection to supervisory investigations and proceedings, under tax privacy provisions, or in pursuit of federal statutes or rules, administrative or judicial proceedings, the legitimate functions of supervisors, and in the case of an emergency related to foreign intelligence or counterintelligence. This law does not apply to state governments, local governments, or private businesses.



## Telecommunications Act of 1996

The Telecommunications Act of 1996 provides regulations for telecommunications carriers that receives or obtains subscriber ownership information. Carriers that receive this information from another carrier may only use the information for the purpose of providing services. The Act explicitly prohibits using this information for marketing purposes. If the carrier receives ownership information through providing services to a subscriber then they can disclose, use, or permit access to the personally identifiable customer ownership network information when they are providing services. The two exceptions to this provision are when required by law or have the consent of the customer. In addition to this the carrier must disclose information to the customer if presented with a written request. However, aggregate data may be disclosed, used, or accessed for reasons other than providing services if access is provided in a nondiscriminatory way. The provisions in this Act do not prohibit information use for the purposes of bill collection or telemarketing practices.

## Video Privacy Protection Act of 1988

The Video Privacy Protection Act of 1988 protects the personal identifiable rental records of prerecorded video cassette tapes or similar audio visual material. These records cannot be disclosed unless it is to the customer or with written consent of the customer. The customer can give consent using electronic means and can give consent for disclosure in advance of said disclosure. Time must be provided for the customer to withdraw from ongoing disclosure. The video provider may disclose if the information only contains the names and addresses of customers. The video provider may also disclose to law enforcement proving they have a warrant for the information. This Act was amended in

2013 to allow video providers to share information with social networking sites with the permission of the customer.

## **2.12 Summary**

Overall, these privacy laws are essentially split into 2 different sections with regards to the privacy protections provided to the public: privacy & information security.

Information security is primarily concerned with the protection of the integrity, confidentiality, and accessibility of data (Amankwa, Loock, & Kritzinger, 2015).

Keeping data confidential is part of protecting online privacy, but information security approaches to laws leave out one very important concept; data collection. Information security's focus is on the protection of the data after collection and during the collection process. This necessitates splitting the laws into two groups based on if they regulate the data that can be collected from users.

The majority of the laws in the United States that relate to online privacy have a central focus on information security. This area of privacy law mainly focuses on how the information collected from users must be used, stored, and accessed. In addition to these core areas the laws also address the disclosure of security breaches to members of the public that are affected. These laws strongly emphasize the importance of maintaining data confidentiality. 13 of the laws have some provision regulating the disclosure practices of information. In general, an entity that collects and stores user data is prohibited from disclosing that data to anyone else without the consent of the user from which the data was collected. Each law has exceptions to this protection with the main exception allowing law enforcement access with a subpoena or warrant. There is not one blanket law that covers information security, instead the laws pertain only to specific

types of institutions or information (financial, health). The more sensitive the information is considered to be, the stronger the privacy protections for the information. For example, any data containing an individual's social security number, or any financial information has some of the strongest privacy protections. Financial institutions under the Gramm-Leach-Bliley Act of 1999 are required to have an information security policy in place that is tested and changed as needed along with a dedicated employee for safeguarding information. These provisions are most likely in place because this type of information can be easily used to commit identity theft. Identity theft in the United States is estimated to affect seven percent of adults and have financial loss exceeding 15 billion dollars (Blake, 2015). Some of the laws with the focus on information security explicitly state in the text of the law that the intent is to protect consumers against identity theft (Computer Fraud and Abuse Act; Consumer Credit Reporting Reform Act).

Another section of the information security laws guard not against identity theft, but against unreasonable search and seizure by the United State government. The privacy laws today extend 4<sup>th</sup> amendment rights to bank records, video records, telecommunication records, medical records, credit reports, unpublished journalistic material, and wire/electronic communications (Communications Assistance for Law Enforcement Act; Consumer Credit Reporting Reform Act; Electronic Communications Privacy Act; Privacy Protection Act of 1980; Right to Financial Privacy Act of 1978; Telecommunications Act of 1996; & Video Privacy Protection Act of 1988). Many of these laws have no specific mentions of the Internet or how information related to Internet use and storage should be treated. At the time many of these laws were enacted the personal computer had not yet reached widespread adoption, let alone the Internet. In

1997 two-thirds of households were found to own a personal computer and on average only had a personal computer for a little less than 2 years (Venkatesh & Brown, 2001). This places the general widespread adoption of personal computers in the mid-1990s which was roughly 5 years after the commercial introduction of the Internet. 9 of the 14 identified privacy laws were enacted before this time, which means there was no reason to consider a technology like the Internet. This omission in the laws force individuals to apply laws enacted under different circumstances to new technologies that may or may not fit within the scope of the law despite the same need for protection.

With one notable exception, all of the laws focusing on information security are only concerned with some form of personally identifiable information. This could coincide with the ability to use the information to commit fraud. The one exception to this is the Electronic Communications Privacy Act which goes beyond protecting personal information and records to protecting the content of communication. This law is the strongest protection that United States citizens have in terms of what can be used against them in the court of law. However, this law does not provide nearly as much protection to Internet users as what it appears to at first glance of the law. This breakdown of protection occurs because of the third party provision. Electronic communications are not protected if a third party is present during the communication. At this time the only form of Internet communication protected under this Act is email because of this provision. A third party is broadly defined as anyone else that can hear, or in the case of the Internet see the communication as it is taking place. Under this definition any web platform is considered a third party since the communication takes place using a service where the provider of the service has the ability to “listen in” on a conversation (Trabsky,

Thomas, & Richardson, 2013). This provision largely leaves the Internet as public space in terms of United States law.

There is only 1 law that qualifies as focusing on the online privacy of individuals in regards to data collection practices which fits with the notion that the Internet is a public space. The Child's Online Privacy Protection Act of 1998 (COPPA) specifies data collection practices of web services for children who self-identify as being under the age of 13. This law was the first true online privacy law in the United States and essentially prohibits the collection of personal information for children under 13 without the consent of the parent (The Online Privacy Protection Act of 1998; Center for Media Education, 2001). The law was amended in 2012 and one of the major updates was significantly changing the definition of personal information. As of 2013 persistent trackers, global positioning information, and a video, photo, or audio file that contains a child's likeness or voice qualifies as personal information (Freeman & O'Neill, 2013). This law is the only privacy law in the United States that includes these pieces of information in the definition of personal information. As a result, many websites prohibit children under the age of 13 from creating an account since data collection practices are highly regulated (Boyd, Hargittai, Schultz, & Palfrey, 2011).

However, there is a very important piece of this law that weakens the privacy protections for children that was added in the 2012 revisions. The law specifies that it only applies to children who *self-identify* as being under the age of 13. There is not a requirement for children to verify that they are over the age of 13 (The Children's Online Privacy Act of 1998), only to check a box or enter a birth date. Today, the result of this law is a large amount of children lying about their age in order to access the desired website (Boyd et

al., 2011). Researchers estimate that there are millions of children with Facebook accounts that are under the age of 13 (Boyd et al., 2011). The addition of this self-identification clause essentially makes this law a piece of paper that is rarely enforced in practice.

There are many different state laws that try to address the gaps in online privacy law. However, most of the states still focus on data security and personally identifiable information over data collection (Russom, Sloan, & Warner, 2011). A few have expanded the definition of personally identifiable information to include information specific to the Internet, more specifically web history. The states that have expanded the PII definition are Minnesota, Arkansas, California, Georgia, Louisiana, and Pennsylvania (Russom et al., 2011). The one state worth singling out is California.

At this time California has been ahead of the rest of the country, including the federal government, in terms of online privacy protections. California passed the first major state online privacy law, the California Online Privacy Protection Act. This legislation was first enacted in 2004 and forced web platforms to display their privacy policies in a place that was easily accessed and noticed by the consumer (California Online Privacy Act; Bergman, Halpert, & Plessner, 2004). This law was amended to include provisions for Do Not Track signatures for California residents and extended the privacy policy requirement to include mobile applications (Donohue, 2014). Do Not Track signatures are essentially a piece of code in a web browser that communicates to web platforms that the user does not wish their online behavior to be tracked (Ferden, 2016; Jaeger, 2013). The law specifically requires web operators to state their response to Do Not Track

signatures, it does not have any provisions that require operators to honor them (Donohue, 2014).

## **2.2 Organization Policies**

The laws in the United States give almost no online privacy protection so the gaps in the laws are filled by organizational policies governed by self-regulation. Many of the privacy laws require that institutions provide notice to their customers as to their policies on data use, collection, and sharing practices. These have typically taken shape as terms of use agreements and privacy policies that vary based on the organization or institution. However, there are not very many laws that govern the use of privacy policies for the majority of online web platforms. The only law that applies to all web platforms is the California Online Privacy Protection Act, which only applies to California residents. Outside of California there is no set requirement that a web platform must have a privacy policy posted unless it falls under one of the regulated industries in the privacy laws put in place before the Internet. Researchers have determined that only 14% of companies that collect user information have a posted privacy policy (Chen & Michael, 2012). Instead of government regulation the Federal Trade Commission advocates for industry self-regulation (Papacharissi & Fernback, 2005). This translates to the web platform having the freedom to include any conditions they want within their privacy policy and require users to agree to these terms before using the web platform.

Web companies are under no obligation to actually protect the privacy of their users through the use of a privacy statement (Papacharissi & Fernback, 2005). Instead the burden is placed on the user to read the posted privacy statement and decide for themselves if they agree to the terms in the privacy policy. This burden has been deemed

unfair by some researchers since privacy policies are written in dense legal language designed to protect web platforms from privacy lawsuits instead of actually informing the user of policies of which they are most concerned (Papacharissi & Fernback, 2005; Pollach, 2007). Even if the privacy policy contained information that the user wanted to know the chance of them being able to comprehend the policy is fairly slim. Research studies that have examined privacy policies for their readability have found that these policies are written above a 12<sup>th</sup> grade reading level with some requiring as much as 2 years of college to fully comprehend (Graber, D'Alessandro, & Johnson-West, 2002; Lewis, Colvard, & Adams, 2008). This is problematic since the Literacy Foundation estimates that up to 50% of adults in the United States cannot read above an eighth grade level (Literacy Project Foundation, 2007).

Compounded with the problems of readability and information included in the statement is the actual length of a privacy policy. Privacy policies can be as short as a paragraph or as long as 15 pages. The amount of time needed to read all of the privacy policies a user would come in contact with in a year amounts to 181 hours per year, assuming that the privacy policies are short. If the privacy policies come closer to the long end of the spectrum an individual is going to spend about 304 hours each year just reading privacy policies (McDonald & Cranor, 2009). This might explain why so many people just skip over the privacy policy altogether. In a small-scale study researchers found that out of 200 users only 7 clicked the privacy policy before signing up for a particular service (Malaga, 2014). On a much larger scale researchers conducted eye-tracking studies to examine how users read privacy policies. The results of the study indicated that when there is an option to agree to the policy without reading it most users will skip reading the



policy (Steinfeld, 2016). Privacy policies are an inadequate way of informing users on the data collection practices of a web platform and do nothing to actually protect the user's privacy.

### **2.3 Recommendations**

At this time the United States approach to online privacy protections is a failure. Legal experts have applied the term "patchwork quilt" to describe the privacy laws in the United States (Diorio, 2015; Soto & Simpson, 2014), but there isn't enough material to construct anything resembling a quilt. The United States one of the only countries with no blanket online privacy laws and also has no regulating body dedicated to data protection (Soto & Simpson, 2014). For the most part the United States has relied on self-regulatory practices for online privacy protection, but organizations have no incentive to protect users' online privacy since personal data is considered a commodity (Hirsch, 2011). In order to negotiate this clash of interests there are different regulatory frameworks the United States could adopt in order to offer greater online privacy protections.

Legal experts in the United States have set forth a structure of four factors for courts to consider when accessing online privacy cases. However, the recommendations are directly related to regulatory practices go back to the self-regulation model using terms of use agreements. The first recommendation is that all entities which engage in communication monitoring or data collection practices online should be required to provide a policy that outlines the specifics of these practices (Haynes, 2012). The theory behind this is that users should be able to find a different service if they do not agree with the statement. This fails to take into consideration that many users are required by

different circumstances to use specific online services. These people would still not have a choice. The second recommendation is that if the user is not provided notice of the privacy policy then they should not be bound by it (Haynes, 2012). This recommendation has some merit, since many online platforms if they provide notification (e.g. Google, Twitter, LinkedIn) only notify the users of significant policy changes. The platform is the one that decides what is “significant” (Google, 2016; LinkedIn, 2014; & Twitter, 2016). However, many users are still left with little action after they agree to a particular policy since holding platforms accountable to their policies can prove difficult (Diorio, 2015). An example of this is the Facebook Mood Manipulation study that was conducted in 2012. Roughly 689,000 Facebook users’ newsfeeds were manipulated to highlight either more depressing or more positive content in order to study the user’s mood change in statuses (Meyer, 2014). However, at the time that the experiment was conducted Facebook’s privacy policy contained no mention of a consent to research. This stipulation was only added 4 months after the conclusion of the experiment (Hill, 2014). When the study was published this news came to light and while the actions of Facebook were deemed to be highly unethical, there was no punishment other than a public relations nightmare. There needs to be a regulatory body that holds web companies accountable to their terms of use agreements and keeps an archive of all versions of a company’s terms of use agreement. For this reason, a hybrid approach to privacy regulation is more suitable than one that is pure self-regulation.

A hybrid approach uses a mixture of industry self-regulation and government regulation to protect online privacy. Part of this regulation is modeled after the European Union’s approach to online privacy. The European Union (EU) has codified a right to privacy and

the data of an individual cannot be handled without permission (Diorio, 2015). There are of course exceptions to this stipulation out of necessity. Instead of the inadequate quilt model of the United States, the EU has universal data privacy laws with one regulatory body overseeing them. This particular approach would simplify the situation in the United States. Currently, the strictest online privacy laws only apply to one state. However, distinguishing between web traffic based on state could be tricky, especially when there are several technologies that can alter Internet Protocol addresses and block geolocation (e.g. TunnelBear, The Onion Router). This would also clarify definitions related to online privacy, such as Do Not Track. At this point in time there is no federal standard for Do Not Track technologies and it is not clearly defined in the California law either (Donohue, 2014).

Individual companies that operate online platforms could still have the ability to set their own terms and conditions, but regulation could help protect individuals from abuse of these documents. One of the ways that privacy policies could be changed is to make certain aspects of data collection and data sharing practices optional. When individuals are given the ability to opt in to certain practices instead of opting out of them by default they are more likely to read the given terms and conditions (Steinfeld, 2016). This would promote transparency and also serve to educate the public about who has access to the data they generate.

The United States has attempted to reform online privacy regulation in the past. In 2012 the Federal Trade Commission released an online privacy report urging for regulation changes to protect the privacy of consumers. The report details a plan for regulation that includes sections on Do Not Track, data broker industry transparency and enforceable

self-regulation (Federal Trade Commission, 2012). The FTC encouraged limitations on data collection and reform of privacy policies that would make them shorter and easier for the average user to understand (Federal Trade Commission, 2012). Many of these recommendations are not out of line with what was proposed earlier. This report drew the attention of industry leaders as well as members of Congress who began to deliberate on sweeping privacy protections (Desai, Drobac, Gates, & Louer, 2012). Around the same time of the FTC report, the White House proposed a Consumer Privacy Bill of Rights that was based on similar principles: transparency, individual control, respect for context, security, access and accuracy, focused collection, and accountability (The White House, 2012). However, this proposed legislation, like many others, never passed. Privacy reform in the United States moves at a glacial pace (Singer, 2016).

### **3.0 Barriers to Greater Privacy Protections**

While the Washington gridlock could partly be blamed for the lack of movement for greater online privacy protections, the issue is far more complex. There are several issues at the heart of impeding privacy protection including industry business models; interests in innovation and research; and motives of law enforcement.

#### **3.1 Industry Objections**

The industry's response to greater online privacy protections is not uniform. In many cases companies will state that they are in favor of greater privacy protections for consumers, but are very specific in the type of protection of which they would be in favor. The information technology industry tends to lean favorably toward greater privacy protections that extend 4<sup>th</sup> amendment protections. A good example of this is the

recent proposal for revising the Electronic Communications Privacy Act. This piece of legislation is largely considered outdated by privacy advocates since it has draconian provisions for email protection against search and seizure (Lofgren, 2014). When a revision of this Act was proposed in 2015 the Computing Technology Industry Association (CompTIA) came out in favor of this legislation (CompTIA, 2015). CompTIA is one of the major lobbying groups for the technical industry and has around 2000 member companies (CompTIA, 2015). However, the industry response changes when proposed regulation is attempting to change the current self-regulation structure in the United States. They frequently state that their objection is due the regulation's likelihood of curbing innovation and research in information technology (Federal Trade Commission, 2012). While this objection is not without merit, there is a greater reason behind their negative position; money.

Currently companies that operate web platforms offer most of their services with no monetary cost for the user. In order to survive, these companies use a similar model to other media industries and depend on advertising revenue. User privacy typically takes a hit since the web platforms collect large amounts of data and then sell that data to advertisers to help them better target their users (Sevignani, 2013). Platforms that collect large amounts of diverse data, like Google and Facebook, are highly attractive to advertisers. Stricter privacy regulations are not favorable for these companies since it would harm their business model. Advertisers were uncomfortable with Google even discussing discontinuing the use of cookies to collect user information (Vranica & Stewart, 2013). After the implementation of stricter privacy laws in the European Union the effectiveness of targeted online advertising diminished. If the same effect would to

be observed in the United States researches estimated that advertisers would have to spend 14.8 billion dollars more in order to reach the same level of advertising effectiveness (Goldfarb & Tucker, 2011). This would seriously devalue online advertising in the United States.

The industry's claim that greater privacy regulation would also harm innovation and research is also a valid point. Online surveillance has helped usher in the era of Big Data which has completely changed some areas of research. Big Data has been defined as large, longitudinal, diverse and complex data sets that can be generated from almost any instrument including click streams, social media, and nearly any digital source (White & Breckenridge, 2014). Today the use of Big Data methodology has increased and is used in a wide variety of fields including medicine, criminology, communication, psychology and education. Instead of researching by taking a sample of a population these data sets come very close to an actual population size which makes it easier to yield statistically significant results (Chan & Bennett, 2016; McCormick, Ferrell, Karr, & Ryan, 2014). This allows for the continued advancement in many fields. Online privacy regulation factors in because many institutions conducting research using Big Data do not necessarily collect their own data. They instead depend on data collected from companies like Facebook and Google (White & Breckenridge, 2014). If these companies were restricted in the amount of information they could collect, it could end up harming research based on Big Data analytics.

### **3.2 Law Enforcement Objections**

The only voice that drowns out the industry's objections is law enforcement. Law enforcement are against virtually any increase in online privacy protections. Greater

privacy protections are in direct conflict with their job since currently the majority of online information has absolutely no 4<sup>th</sup> amendment protection. This makes it much easier to gain information necessary for criminal investigations, prosecution, and in some areas prevention. Law enforcement is even against greater privacy protections that do not directly regulate them which includes any protection that would limit data collection and enhance data security. This reasoning behind this objection goes back government surveillance practices under the Patriot Act.

The Patriot Act is a massive piece of legislation with 1041 sections that was passed shortly after the September 11, 2001 terrorist attacks. The main purpose of this Act was to give the government all the power necessary in order to combat the threat of terrorism. The Patriot Act greatly expanded the legality of surveillance programs in the United States and was one of the first pieces of legislation to greatly expand that power (USA PATRIOT Act, 2001). In 2008 the government's power was further expanded and this expansion is responsible for the birth of the PRISM program (Ahn, 2014). This program remained secret up until 2013 when Edward Snowden leaked classified National Security Agency (NSA) documents to The Guardian (Toxen, 2014). These documents revealed that the PRISM program allowed the NSA to collect massive amounts of user information including video, pictures, audio, emails, documents, and connection logs directly from major technical companies (Gray & Citron, 2013). The NSA collected from data from some of the largest Internet platforms including Google, Facebook, YouTube, and Yahoo (Florek, 2014). The fact that these companies were already receiving and collecting massive amounts of information made collection for the NSA much easier. If these companies did not collect as much information, or the information

was more secure the program could have been more difficult to execute. Both law enforcement and the information technology industry work together to lobby against greater online privacy protection through the form of regulation. Congress is still hesitant to enact greater privacy protections through regulation. Many of the entities that have weighed in on the regulation discussion have proposed an alternative to protecting the online privacy of users by shifting the burden of protection on to the users themselves.

#### **4.0 Privacy Enhancing Technologies**

The Federal Trade Commission in their 2012 report on privacy advocated for greater privacy protections in the form of regulation, but also advocated for users to utilize privacy enhancing technologies such as encryption. There are several techniques available to users today that can help them take charge of their own online privacy instead of waiting for regulation that may never happen. These techniques vary in the amount of skill and technology required to use them. Some privacy enhancing techniques rely less on technology, but more on changing habits online. There are a variety of techniques available for users to protect their own privacy online, but which technique they decide to use will be dependent on the type of privacy protection they desire. None of these techniques have the power to extend 4th amendment rights to online information, only the law has that power. In general, these techniques work in one of two ways: preventing data collection or changing the content of the information in a way that makes it useless to the collector thus it is important to understand how information can be collected. There are three easily distinguishable ways that information can be collected online. The first method of data collect most Americans are aware of at this point and that is voluntary disclosure. Anything that is willingly put online is



typically collected by someone. There are two other methods of collecting data that users need to be aware of in order to choose techniques to protect their privacy: cookies, web bugs.

#### **4.1 Data Collection Methods**

Cookies are small pieces of text that are stored on a user's browser that are used to identify that browser if they should visit the site again (Yue, Xie, & Wang, 2007). Over time there have been many different developments in cookies that vary on use and longevity. Some cookies are very useful, such as the ones used for transaction oriented data, vanish as soon as the web browser is closed (session cookies), those that can store passwords so they don't have to be memorized as well as those that personalize a user's web experience (Yue, Xie, & Wang, 2007). Cookies can also be seen as a violation of privacy since this technology can also enable the tracking of users across multiple sites and by using the site the user could be implicitly agreeing to the use of cookies (Berghel, 2013). The use of tracking cookies by advertisers is fairly widespread at this point. Researchers found that there is more than a 99.5% chance that if a user visited 30 results of a search engine inquiry they would be subjected to the tracking of at least 10 different cookies (Gomer, Rodriegues, Milic-Frayling, & Schraefel, 2013). The good news is cookies can easily be deleted by the user on a fairly regular basis and their use is fairly well known (Goldfarb & Tucker, 2011).

This brings up the next method of data collection which is web bugs. Web bugs are small pieces of code embedded in a website that are invisible to users (unless one decides to examine the code itself) (Goldfarb & Tucker, 2011). This code works in conjunction with cookies to track a user's habits as they travel from site to site. Essentially the purpose of a

web bug is to track the user's web navigation (Fonesca, Pinto, & Meira, 2005). Web bugs pose a new challenge to privacy since they are invisible to the user and are not stored on the user's computer at all (Goldfarb & Tucker, 2011). Most users are probably not aware that these pieces of code exist at all, which makes it very difficult to fight against them.

## **4.2 Types of Data**

In addition to there being multiple methods of collecting data online, there are multiple types of data that can be collected and are they not treated equally by privacy enhancing technology. There are roughly five types of data which are mainly collected by commercial entities: user content, meta data, web navigation, search, and clickstream data. User content is the type of data that most people will first think of. This type of data encompasses anything a user would post online including videos, audio chats, pictures, social media posts, and emails. Meta data is essentially data that describes the user's post itself, not the content in the post. This can cover many pieces of information such as Internet Protocol address, geolocation data, name, time stamp, etc. Web navigation and search are types of data that are fairly self-explanatory. Web navigation is a user's movements from website to website, so essentially a browsing history that includes every link clicked as well as that typed in. Search data is anything typed in to a search engine. Clickstream data is slightly more complex. When a user is interacting with a website every click they make on the page is considered to be clickstream data along with how they arrived to that page, and how long they spent on it (Goldfarb & Tucker, 2011).

Each of the privacy enhancing technologies will be analyzed according to what type of protection they provide, the type of information they protect, and the ease at which the user can pick up the technology. There are five broad categories of technology that seek to provide greater privacy protection for users: Tracker blockers, private browsers, encryption technology, self-destruct tools, and anonymity technology.

### **4.3 Privacy Enhancing Technologies**

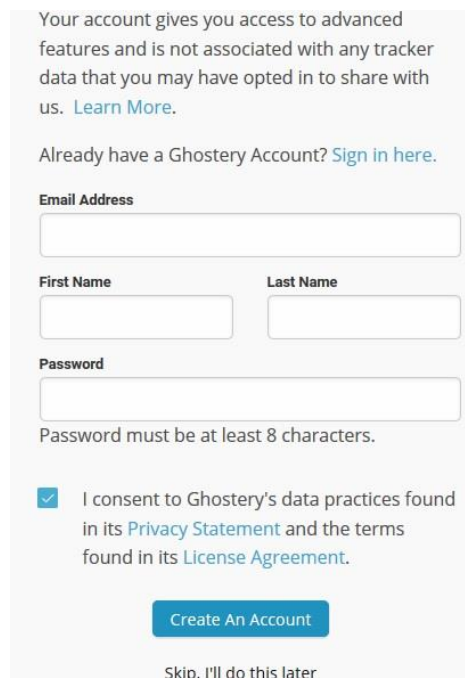
#### Tracker Blockers

This technology is based on a tool developed in 2005 to detect Web Bugs. A Web Bug detector intercepts a Hypertext Transfer Protocol (HTTP) requests from both the user and the website in question and analyzes those requests. By comparing the user request with the response from the website the technology is able to detect the presence of any Web Bugs. This detector was designed to make users aware of these invisible privacy invaders and turns red when a Web Bug has been found (Fonseca et al., 2005). Tracker blockers go a step further by not only detecting Web Bugs, but also eliminating them. The elimination is accomplished by not showing the content that contains the Web Bug. In addition to finding and eliminating Web Bugs, tracker blockers also locate and block cookies that exist for the sole purpose of tracking user behavior (Chen & Singer, 2016). Tracker blockers work by protecting the user against data collection, it does not eliminate the data itself, which means if the trackers ever surpass the technology blocking them then the user's privacy is in jeopardy. This technology mainly protects navigation data and offers little to no protection outside of that ability. Most of the tracker blockers on the market today are available for free and come in the form of a browser extension which can be installed with just a few clicks. Very few of the individual technologies

fully explain how they work, but this might be to limit the technical jargon in the extension. At this point there are lots of tracker blockers on the market but there are three that have risen above the rest of the market: Ghostery, Disconnect, and Privacy Badger. Each of these specific technology offers a different approach to privacy.

Ghostery is by far the most popular tracker blocker at this point with over 40 million downloads and is an extension available for Chrome, FireFox, Safari, Internet Explorer and Opera. Ghostery maintains a database of web trackers totaling to over 2000 trackers (Ghostry). This extension takes some time to set up since by default it blocks absolutely no web trackers. For those highly concerned with privacy it may not be the best tool to use since it actually collects data from its users in order to help maintain its database. While this feature is available in the form of “opt-in”, it is a little concerning to see user data collection from a privacy enhancing technology. Following the screen that requests

Figure 1. Ghostery sign up screen



Your account gives you access to advanced features and is not associated with any tracker data that you may have opted in to share with us. [Learn More.](#)

Already have a Ghostery Account? [Sign in here.](#)

**Email Address**

**First Name** **Last Name**

**Password**

Password must be at least 8 characters.

I consent to Ghostery's data practices found in its [Privacy Statement](#) and the terms found in its [License Agreement](#).

[Create An Account](#)

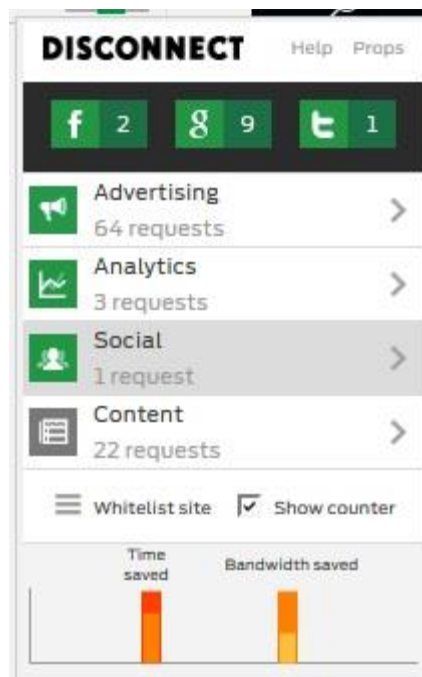
[Skip, I'll do this later](#)

the user to opt-in to tracking is a screen requesting the user to create an account, consent to data sharing practices, and consent to their privacy statement which can only be reached by following another link (see Figure 1).

Once all the hoops are jumped the extension is not that difficult to use, but requires the user to essentially customize the blocking procedures for every single site (Ghostery). Developers stated that this was done by choice since blocking some trackers can essentially break a site (Chen & Singer, 2016). This could potentially be very exhausting for those that use the Internet on a fairly regular basis. The biggest hurdle to get over with Ghostery is that it is a privacy enhancing technology that engages in the same practices as the industry does by collecting data from its users and requesting user information up front. Some of the reviews of the new release in March 2016 also accuse the site of some shady business practices which include deleting most of the negative reviews on their product (Mele20, 2016). Disconnect is another tracker blocker that is a fairly popular choice for web users, but it goes a step further in terms of protection compared with Ghostery. Disconnect offers three versions of its main technology. The two more advanced versions of Disconnect are available for a fee, but also double as malware protection so there is more there than just a tracker blocker. This analysis will focus on the basic version which is available to users at no charge. Disconnect has an easy to understand interface (see figure 2) with a useful tutorial at the beginning. Unlike Ghostery, this extension comes with some trackers blocked by default and collects absolutely no user data. Instead of maintaining a database of known trackers Disconnect keeps track of how many requests are made to the browser and automatically blocks everything from advertisers, analytics, and social media. The only tracker that is kept on

by default are those that relate directly to the content of the site. If the same tracker makes multiple requests, it will count each of those requests separately on the counter. One of the interesting features of Disconnect is that it allows the user to see all of the bandwidth and time saved by blocking the tracking requests, but there is no information on how either of those numbers is calculated (Disconnect).

Figure 2. Disconnect Interface



Privacy Badger is the third tracker blocker and takes a very different approach compared to the other two blockers. Privacy Badger was developed by the Electronic Frontier Foundation, one of the biggest privacy groups in the United States. The goal of Privacy Badger is not to block every tracker on a web page, but instead to enforce a Do Not Track signature. Remember, Do Not Track signatures are identifiers in a web browser that signal to other sites that the user does not wish to be tracked (Ferden, 2016). The way Privacy Badger operates makes it a far more sophisticated tool than the other two, but possibly more difficult to use as well. Privacy Badger requires no setup when the

browser extension is installed and it blocks absolutely nothing at that point. After enabling the browser's Do Not Track signature, Privacy Badger identifies all *potential* trackers on a web site, but it does not block any of them unless it actually sees them track the user. The way this works is that Privacy Badger maintains a list of potential trackers from one site and if the same potential trackers appear across multiple sites they are flagged as trackers and blocked (Electronic Frontier Foundation, 2015). Any site that has language written in to their policies stating that they will honor Do Not Track signatures will not be blocked, which leads to some confusion with users (Broida, 2014; Chen & Singer, 2016). Privacy Badger learns what to block over time and becomes more useful the longer it is used, which is something that is not seen in either of the other two tracker blockers.

Privacy Badger's design is more complex and difficult to understand than the other two tracker blockers. Each potential tracker has a slide bar next to it that changes from green, to yellow, to red, depending on the status of the tracker (see figure 3). If the bar is green the domain is allowed, if it is yellow the domain has been identified as tracking the user but it is necessary for some type of content on the page, and red signals that the tracker has been blocked. Instead of giving the names of the sites responsible for the trackers like Disconnect and Ghostery, Privacy Badger gives the exact Uniform Resource Locator (URL). This could make it harder for users to understand the nature of the interface if they do not automatically know what companies the URLs are associated with. In addition to the confusing slider configuration there is a separate section of the extension that identifies sites that "do not appear to be tracking you" which are always allowed. However, no further explanation is given regarding sites that fit in that category

anywhere in Privacy Badger's information or frequently asked question section (Electronic Frontier Foundation).

Figure 3. Privacy Badger interface



## Private Browsing

Private browsing is possibly the simplest technique that someone can use to protect their online privacy. Private browsing protects the user's identity from other websites and ensures that no data from the session is stored on the user's hard drive. The information is still recorded during the session, but deleted after the private browsing window is closed (Ohana & Shashidhar, 2013; Zhao & Liu, 2015). Many popular web browsers have some form of private browsing option at this time with the most notable browsers being Chrome, Firefox, and Safari. Private browsing generally protects privacy in two ways, by preventing some collection of data, but also removing the data itself. Generally



private browsing can protect a user's web navigation and search data. The protection does not necessarily extend to the other 3 types of data because the collection mechanism could include the website itself and not just third party cookies and bugs. While private browsing is one of the easiest ways to protect online privacy, it is not guaranteed to work in all circumstances. Researchers have found that the use of web extensions in a private browser can compromise the security in the private browser (Zhao & Liu, 2015). Users who choose to utilize private browsing as their main form of privacy protection should refrain from using extensions at the same time, which means that private browsing cannot be used in conjunction with tracker blockers.

## Encryption

Encryption technology is one of the strongest privacy enhancing technologies to date. Encryption methods use a mathematical algorithm to encode the data, with the result being unreadable unless the ciphertext is decrypted using a key (Saitta, 2015). Privacy enhancing technologies that use encryption are the strongest methods available for protecting information. This strength is necessary since encryption based methods are used for more than just protecting privacy, but also for securing highly sensitive information. In the privacy laws that cover financial information and data security there are provisions that require the use of encryption for certain information (Privacy Act of 1974). This is because encryption is very difficult to break for all parties that do not possess the key (Spafford, 2016). Encryption technologies are the only technologies that cross over into granting some protection from law enforcement. In order to access the information authorities typically have to possess the key and the courts have found that an individual cannot be compelled to surrender encryption keys because it violates the 5<sup>th</sup>

amendment right against self-incrimination (Atwood, 2015). The available privacy enhancing tools that use encryption protect user content and not necessarily any other form of data. The most common technologies are emailing and messaging systems. After the Snowden leaks many email messaging systems started to pop up that claimed they were immune to NSA spying. These systems all have a few commonalities, mainly they offer end to end encryption with servers located outside of the United States, for free. The two most vetted free encrypted email services are Tutanota and ProtonMail.

### Tutanota

Tutanota launched its testing phase in 2011 with the service opening its doors to everyone in 2014 (Infosecurity, 2014). The email service is based in Germany and offers end to end encryption with a gigabyte of storage (Prabhu, 2016). No one at the company has access to any of the user's data because of how the encryption keys are stored. The downside to this level of security is that there is no password reset button or help if a user is locked out of their email. All data associated with the email including subject lines and attachments are also encrypted. A user that receives an email from a Tutanota address has two options for reading the contents. If the user receiving the email also has a Tutanota address, then the user can decrypt the email by logging into their account. However, if email is sent to a non-Tutanota address instructions on how to decrypt the message must be sent through a different channel such as text messaging (Infosecurity, 2014). The email system is fairly straight forward and the signup process is very easy. The hardest parts of using this particular service is the necessity of remembering the password entered when creating the account and sending encrypted email to those not using Tutanota.

## ProtonMail

ProtonMail is a Switzerland based encrypted email service that was launched in May 2014 and was exclusively an invite-only service for two years. The service was developed by scientists from the European Organization for Nuclear Research following the Snowden revelations. The service just ended its beta trial in 2016 and started open registration in March of 2016 (Martin, 2016). This service adds another layer of security to the Tutanota design by requiring two separate passwords in order to access email. The first password authenticates the user to the server and a second password is required to decrypt the email once logged on. Like Tutanota, none of the password information is stored on the server, so if a user forgets their password there is no recovery system (Grauer, 2015). Switzerland's data privacy laws are some of the strictest today, and their claim of protecting their users' privacy has already been tested by the United Kingdom. ProtonMail can only turn over information if they receive the order from a Swiss court approved by a judge, and even then it can only hand over the information in its encrypted form. This is exactly what happened when law enforcement agents reached out to ProtonMail earlier in 2016, they simply do not have the ability to decrypt the information which makes them out of the reach of law enforcement at this time (Theilman, 2015). Overall the service is more clunky than Tutanota and requires more effort on the part of the user because of the two password verification system. The service is fairly slow and still has the same problems with sending external emails. Unless a user has the need to greater security, Tutanota would be the easier of the two systems to use.

In addition to encrypted email providers there are also a few instant messengers available that use encryption to keep communication secure between two people. At this time

encrypted instant messengers are fairly new, so there are not many out that are highly user friendly. The most well-known encrypted instant message systems at this time is Off the Record (OTR) Messaging.

### OTR Messaging

OTR Messaging is actually a plug-in that can be used with other instant messaging services which makes it one of the most versatile tools available. OTR uses symmetric encryption, which only requires one key for decrypting messages. To solve the key-sharing problem that occurs with symmetric encryption the plug-in uses a modified version of the Diffie-Hellman exchange protocol which was initially developed in 1976. The Diffie-Hellman protocol is not the most secure way to exchange keys as it is vulnerable to replay and man-in-the-middle attacks (Li, 2010). However, the message must be targeted in order to use either of those attacks, which is not likely in most circumstances with an instant messaging system. OTR was specifically designed to be easy to use since poor usability is one of the main reasons strong privacy enhancing technologies have poor adoption (Stedman, Yoshida, & Goldberg, 2008). This plugin is activated using a button in an instant message client (currently the only one supported is Pidgin) and communicates to the user the status of the conversation in regards to privacy. There are possible statuses of a chat: not private, unverified, private, and finished. If the chat is not private that means that the other user has not enabled OTR. If the chat is unverified then the other user has not been authenticated, so the user may be talking to someone that is not on their buddy list. A private chat is exactly that-private. A chat is marked finished when one or both of the users closes the chat window (Stedman et al., 2008). There are a couple of methods that can be used for authentication, either the users

share a secret with each other, or use a fingerprint. The shared secret is a piece of information that both users know, but few others would know (Stedman et al., 2008). An example of this would be using either the date, time, or location of their last in person meeting. If the answers match, then the chat is authenticated.

Currently there are a few messaging systems directly supported by OTR, but one of the easiest to configure is Pidgin. Pidgin is an instant messaging client that allows the user to sign in to all supported instant messaging accounts from one place (e.g. Yahoo!, AIM, XMPP). In order to use Pidgin the user must have an instant messaging account already

Figure 4. Off The Record plug-in button in Pidgin



from some other provider. To use the OTR plug-in the user must first download it from the OTR site since it is not built in to Pidgin and then once installed enable the plug-in for use. Once OTR has been enabled it is fairly easy to use. To start OTR within a chat the user would click the small button at the bottom of the window (see Figure 4).

From there a small drop down menu would appear with options to start a private chat. If both members of the conversation already have private chat enabled, then there will be an option to authenticate the user (see Figure 5).

Figure 5. Off The Record plug-in drop down menu



The authentication option brings up a screen that is easy to navigate and gives option as to how the user wants to authenticate their “buddy”. Once the authentication is complete the users are free to engage in a chat protected by encryption. The hardest part of this plug-in is knowing where to find it and install it. The rest of the information is readily available if the user has questions when attempting to use the plug-in for the first time.

#### Self-Destructing Emails/Messages

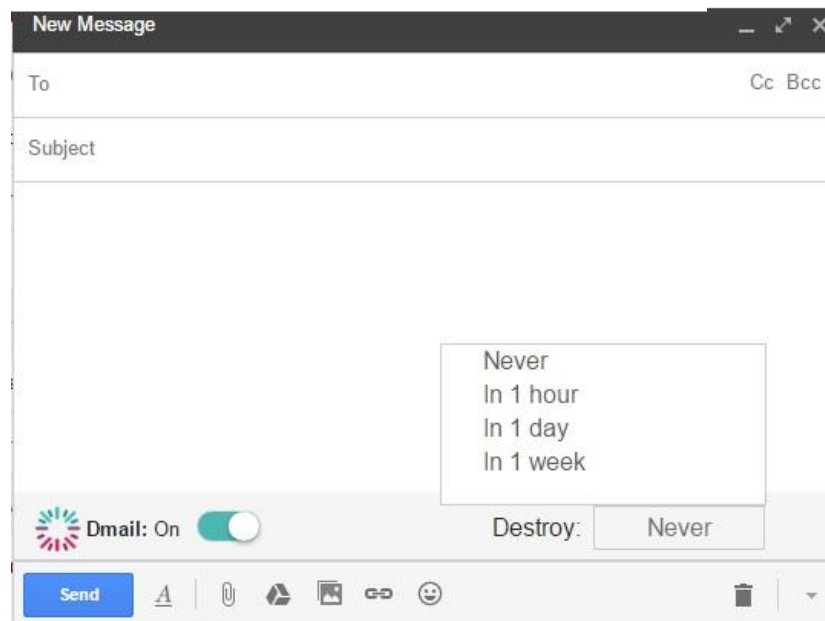
Self-destruct is a type of privacy enhancing technology ensures that information is completely deleted with no traces after either an expiration time or after the recipient reads the message. When an email is deleted, it still remains in the system of the email provider, even if the message has been deleted by all recipients of the message (Fu et al., 2014). The same can be said for any electronic communication. All records are kept by the provider unless it is stated otherwise in the terms and conditions. An email or message can self-destruct by becoming completely unreadable (Fu et al., 2014). This self-destruct mechanism can be accomplished in many ways and there have been numerous protocols proposed for self-destructing data (Fu et al., 2014; Yue, Wang, & Liu, 2010; Zing, Shi, Xu, & Feng, 2010). As such, there are multiple privacy enhancing tools that use self-destruct technology. Because self-destructing technology is so common, it is difficult to identify which tools are the best for an individual to use. The

majority of tools freely accessible to users do not identify how their messages self-destruct or provide documentation showing that it works. To better illustrate how self-destructing tools function 2 tools were selected based on their differences in uses: Dmail, and Privnote.

## Dmail

Dmail is a browser extension that gives the user the ability to revoke access to emails sent through their Gmail account. When the user installs the Dmail extension each new message has a new option called “Destroy” that appears in the lower right hand corner of the new message (see Figure 6). From there the user can choose when they want the message to self-destruct (never, 1 hour, 1 day, or 1 week).

Figure 6. Dmail function within Gmail



## Privnote

Privnote is another self-destructing technology that is specific to messages. Privnote is a bit more versatile than what Dmail and other self-destructing emails tools because it concentrates only on the text the user wants to self-destruct. In order for a user to send a self-destructing message using Privnote they would enter their message in a simple online form and click “create message” (see Figure 7). After creating the message, the user will be given a link that they can share with who they want and however they want. When the link is clicked it will display the chosen message and the message will no longer be accessible after the window is closed.

Figure 7. Privnote online form



The image shows a web form for creating a note. At the top left, it says "New note" in bold. To the right of this is a small square button with a question mark. Below the title is a large yellow rectangular text area with the placeholder text "Write your note here...". At the bottom left of the form is a red button with the text "Create note" in white. At the bottom right is a grey button with the text "Show options".

### 4.31 Anonymity technology

In addition to the privacy enhancing technologies discussed previously in this section, users also have the option to adopt an anonymity technology in order to protect their online privacy. Anonymity technology focuses on making sure that the user’s identity remains unknown by ensuring that the data associated with the online activities cannot be linked back to the user in any way (e.g. IP address, name, geolocation) (Winkler &



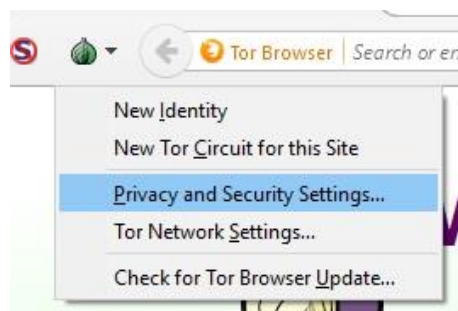
Zeadally, 2015). This definition goes a step further than how many social science researchers view anonymity by discussing the data along with how other users would view the individual using the tool (Morio & Buchholz, 2009). Unlike the other privacy enhancing technologies, an anonymity technology does not protect the user against data collection, or ensure that the content or data is unreadable to anyone that collects it. Because of this major difference, experts have debated if this technology truly protects a user's privacy. If any entity was able to deanonymize the data, then the user's privacy is immediately compromised (Shmatikov, 2011). However, since anonymity as a means of privacy is becoming a more common approach to managing online privacy there is one selection of tools worth mentioning: The Tor Project. The Tor Project provides many different anonymity technologies and is included in this work because its high level of security and user base makes it less likely that its traffic would be deanonymized if it was used correctly (Hoang & Pishva, 2014; Ruiz-Martinez, 2012).

## Tor

Tor is an anonymity technology that is based on onion routing. Onion routing is a method of routing message packets that uses layers of encryption. The message is routed through a series of nodes before it reaches the intended recipient. The path that the message takes to the recipient is encrypted where each node only knows the next point in the path (Hoang & Pishva, 2014). This severs the link between the sender of the message and the message itself. Tor currently has multiple technologies that are based on this technology, but the two more pertinent to privacy are the Tor browser and Tor messenger. The Tor browser can be downloaded for free and operates like a typical web browser. When a user first opens the browser it assigns them a different IP address from

their own, and then using onion routing for all traffic. Any information that might be collected during that browsing session (including user content) will not be able to be linked back to the user. The exception to this is if the user gives away any information during their communication with others that could be traced back to them (e.g. email address). This protection is offered in the default setting, however, if the user wants more security they have the option to change the settings. To do this they would click on the onion icon in the top left hand corner of the browser and click on privacy and security settings (see Figure 8).

Figure 8. TOR browser menu

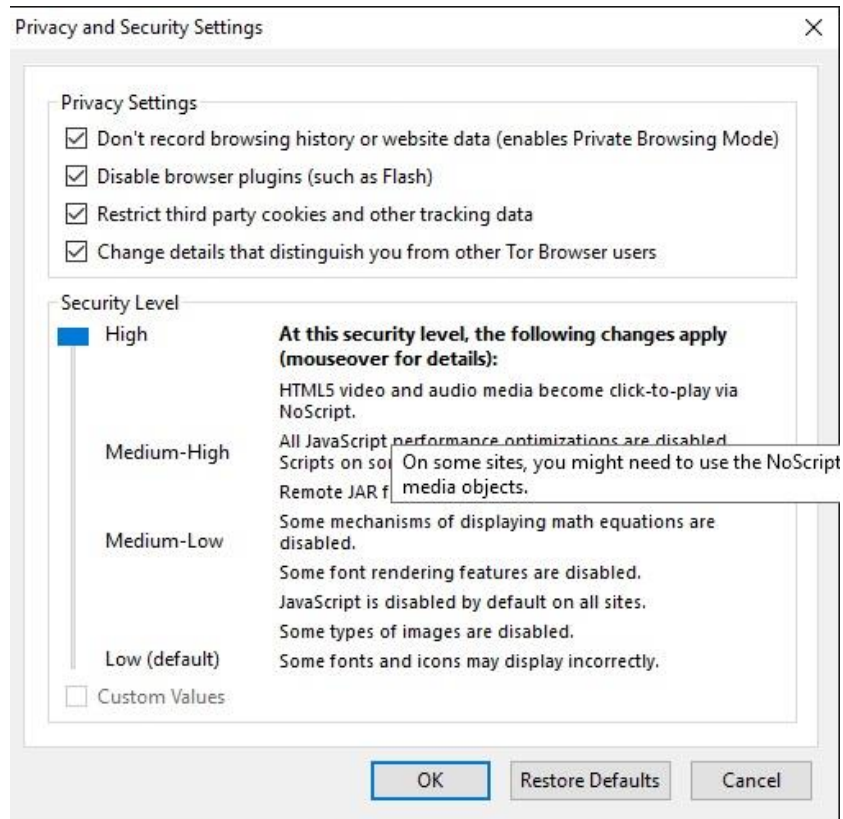


This will bring up a menu of security options. If the highest level of security is selected, the browser will also function as a tracker blocker as well as an anonymity technology (see Figure 9).

Tor messenger is relatively new to the Tor family and gives the ability for users to chat anonymously, but also encrypts the contents of the chat which makes it both a privacy enhancing technology by the strict definition as well as an anonymity technology. The client essentially takes the OTR encryption protocol and then routes all of the information over Tor (Greenberg, 2015). Other than that, it operates exactly as the OTR messaging

system does for now. At this time the Tor messenger service is still in beta, so how this format changes over time remains to be seen (sukhbir, 2015).

Figure 9. TOR privacy and security setting levels



## 5.0 Discussion

When examining the state of online privacy today in the United States there are a few commonalities between the protections provided legally and through technology. The main commonality is that both legally and technically there is almost no protections against data collection. The closest protection against data collection offered in the privacy enhancing technology are the tracker blockers. However, from a technology

standpoint this is understandable since it is difficult to safeguard data against collection when the Internet is a very public place. This is an area where the law is expected to step in, but that is not likely to happen given that both the government and industry have a vested interest in keeping data collection alive and unregulated. Imposing data collection regulations in the United States could have a much greater impact than in any other nation since the majority of Internet companies are located in the United States. While many of these have expanded internationally at this point, the United States is the major powerhouse in terms of Internet innovation and startups. Since so many industries have a dependence on the current data collection practices it could be causing a chilling effect on any developments in law or technology.

Data security is also an area that is far more advanced in both legal protections and technological protections. This area has a history of a strong government interest since data security is necessary for classified operations. Because of this dependence more time, energy, and money has been spent into developing protections in this area. A good example of this in practice is encryption. Encryption is the basis of the strongest privacy enhancing technologies but it also happens to be at the heart of making many online activities secure. At this point in time encryption is used for every online financial transaction, user authentication, and in most email communication. Because this technology is necessary for every day security it is constantly being improved. Those improvements in turn benefit online privacy because developers can use the same methods for privacy technologies.

Protecting online privacy in the United States will remain one of the most difficult tasks to manage given the barriers against greater regulation complexity of the issue. This will

become more difficult to manage as the line between online and offline becomes less distinct. At this point in time more devices are by default connected to either the Internet or a mobile network including televisions, fitness trackers, and other smart technology. If the law continues to update at a glacial pace compared to the development of new technology, then soon most of the current privacy protections will no longer be applicable. If technology keeps developing at this pace, then users will be left to manage their own privacy using technology or other means.

### **5.1 Limitations & Future Research**

This research was very focused in that it concentrated the United States and Internet accessed through desktop computers. This focus left out online privacy on an international scale, mobile technology, and other devices that connect to the Internet. Each of these areas have unique privacy concerns that are worth addressing. Online privacy on an international scale is difficult to discuss since each country approaches privacy differently according to the nature of culture and governmental structure.

However, since the Internet very rarely discriminates between nations it is becoming increasingly important to discuss online privacy on an international level. Specifically, there is a lot of room for research on how privacy disputes are handled across international borders and the potential impact of international privacy standards.

Mobile technology in particular is one of the larger areas that needs to be addressed in future research. This area was left out of the current research due to how fundamentally different the privacy protections are from desktop Internet access. Currently mobile technologies rely on apps for many of the customizable functions. These apps are still highly controlled by the major players in the mobile industry with little room for third

party development and adoption. This is a completely different playing field from that of desktops where there are little limitations on what technology can be used other than the operating system. Future research should focus on how privacy enhancing technologies have developed for mobile devices as well as how terms and conditions are implemented in mobile apps.

## 5.2 Conclusion

The United States has a long way to go in terms of protecting online privacy. The majority of the legal protections are laws that were enacted long before the Internet was commercially available and were just applied to the Internet as if it were any other technology. With no federal law protecting privacy on a universal level for adults, there is room for improvement. The burden of protecting online privacy has fallen to the user who is expected to read an obscene amount of text found in terms of use agreements and determine how to respond if they do not agree with the terms presented to them. If they do not agree, but have no choice but to sign or didn't read the terms until after they already signed the agreement they are left to using technological means to protecting their privacy. Overall, situation in regards to protecting online privacy in the United States is grim. While there is most certainly room for improvement, it may take over a decade before any true progress is made. Until then, the best hope for privacy is that the technological protections outpace the threats to online privacy.

## References

- Ahn, J. (2014). Seizure of electronic data under USA PATRIOT Act. *Seton Hall University Law Student Scholarship*. Retrieved from [http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1434&context=student\\_scholarship](http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1434&context=student_scholarship)
- Albanesius, C. (2010, June). Consumers haven't learned not to divulge private info online. *PC Magazine*, 29(6), 1. Retrieved March 16, 2016 from Ebscohost.
- Amankwa, E., Loock, M., & Kritzinger, E. (2015). Enhancing information security education and awareness: Proposed characteristics for a model. *2015 Second International Conference on Information Security and Cyber Forensics*, 72-77. doi: 10.1109/InfoSec.2015.7435509
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9), 5. doi: <http://dx.doi.org/10.5210/fm.v11i9.1394>
- Berghel, H. (2013). Toxic cookies. *Computer*, 46(9), 104-107. doi: 10.1109/MC.2013.330
- Bergman, A., Halpert, J. J., & Plessner, R. (2004). California law requiring web sites and online services to post a privacy policy goes into effect July 1, 2004. *Venulex Legal Summaries*, 1-4.
- Blake, A. (2015, September 28). Identity theft affected 17.6M, and cost \$15.4B in 2014: The Justice Dept. *The Washington Post*. Retrieved from <http://www.washingtontimes.com/news/2015/sep/28/identity-theft-affected-176-million-cost-154-billi/>
- Boyd, D., Hargittai, E., Schultz, J., Palfrey, J. (2011). Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act'. *First Monday*, 16(11), 1-22.
- Brioda, R. (2014, October 17). Six browser plug-ins that protect your privacy. *Computerworld*. Retrieved from <http://www.computerworld.com/article/2692560/six-browser-plug-ins-that-protect-your-privacy.html?page=2>
- Cable Communications Policy Act of 1984, Pub. L. 98-549, 98 Stat. 2779. (1984).
- California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2003).
- California Security Breach Information Act, Cali S. B. 1386, (2002).
- Center for Media Education (2001). *COPPA (Children's Online Privacy Protection Act): The first year--a survey of sites. A report on website compliance*. Retrieved from

Center for Media Education website  
[http://www.cme.org/children/privacy/coppa\\_rept.pdf](http://www.cme.org/children/privacy/coppa_rept.pdf).

- Chan, J. & Bennett, L. M. (2016). Is big data challenging criminology? *Theoretical Criminology*, 20(1), 21-39. doi: 10.1177/1362480615586614
- Chen, X. & Michael, K. (2012). Privacy issues and solutions in social network sites. *IEEE Technology and Society Magazine*, 31(4), 43-53. doi: 10.1109/MTS.2012.2225674
- Chen, B. X. & Singer, N. (2016, February 17). Free tools to keep those creepy ads from watching you. *The New York Times*. Retrieved from <http://www.nytimes.com/2016/02/18/technology/personaltech/free-tools-to-keep-those-creepy-online-ads-from-watching-you.html>
- Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2681. (1998).
- Communications Assistance for Law Enforcement Act of 1994, Pub. L. 103-414, 108 Stat. 4279, (1994).
- CompTIA (2015, December 1). 29 state and regional tech councils join CompTIA and TECNA urging Congress to pass ECPA reform. Retrieved from <https://www.comptia.org/about-us/newsroom/press-releases/2015/12/01/29-state-and-regional-tech-councils-join-comptia-and-tecna-urging-congress-to-pass-ecpa-reform>
- Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 et seq., (1986).
- Consumer Credit Reporting Reform Act of 1996, 15 U.S.C. § 1681 et seq.,(1996).
- Desai, M., Drobac, M., Gates, M., & Louer, G. (2012). The FTC privacy report and the White House consumer privacy bill of rights: Policy making trends and what you need to know in 2013. *International Journal of Mobile Marketing*, 7(3), 66-81.
- Diorio, S. (2015). Data protections laws: Quilts versus blankets. *Syracuse Journal of International Law and Commerce*, 42(2), 486-513.
- Disconnect (n.d). Disconnect. Retrieved from <https://disconnect.me/disconnect>
- Donahue, M. (2014). Changes to the California Online Privacy Protection Act. *Intellectual Property Litigation*. Retrieved from Ebscohost.
- Duggen, M., Ellison, N. B., Lampe, C., Lenhart, A. & Madden, M. (2015, January 9). *Social media update 2014*. Retrieved March 15 2016 from Pew Research Center website <http://www.pewinternet.org/2015/01/09/social-media-update-2014/>
- Electronic Communications Privacy Act, 18 U.S.C. § 2510-22 (1986).
- Electronic Fund Transfer Act, Pub. L. 95-630, 92 Stat. 3641 (1978).



- Electronic Frontier Foundation (2015, August 6). Privacy Badger 1.0 blocks the sneakiest kinds of online tracking. Retrieved from <https://www.eff.org/press/releases/privacy-badger-10-blocks-sneakiest-kinds-online-tracking>
- Electronic Frontier Foundation (n.d.). Privacy Badger. Retrieved from <https://www.eff.org/privacybadger>
- Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1974).
- Federal Trade Commission (2012, March). Protection consumer privacy in an era of rapid change (FTC Report). Retrieved from <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>
- Ferden, K. (2016). The Swanson paradox: Do-not-track and the intersection of data autonomy and the free market. *Journal of Corporation Law*, 41(2), 493-508.
- Florek, A. (2014). The problems with PRISM: How a modern definition of privacy necessarily protects privacy interests in digital communications. *The John Marshall Journal of Information Technology & Privacy Law*, 30(3), 571-606.
- Fonesca, F., Pinto, R., & Meira, W. (2005). Increasing user's privacy control through flexible Web bug detection. *Third Latin American Web Congress*. doi: 10.1109/LAWEB.2005.19
- Freeman, D. R. & O'Neill, J. (2013). FTC issues substantially revised COPPA rule effective July 1, 2013: Review of changes and compliance tips. *Venulex Legal Summaries*, 1-8.
- Fu, X., Wu, H., Yang, J. Q., & Wang, Z. Z. (2014). How to send self-destructing email: A method of self-destructing email system. *2014 IEEE Congress on Big Data*, 304-309. doi: 10.1109/BigData.Congress.2014.51
- Ghostery (n.d.). Ghostery. Retrieved from <https://extension.ghostery.com/intro#start>
- Goldfarb, A. & Tucker, C. E. (2011). Privacy regulation and online advertising. *Management Science*, 57(1), 57-71. doi: 10.1287/mnsc.1100.1246
- Google (2016, March 25). Privacy policy. Retrieved March 30, 2016 from <https://www.google.com/intl/en/policies/privacy/?fg=1>
- Gomer, R., Rodrigues, E. M., Milic-Frayling, N., & Schraefel, M. C. (2013). Network analysis of third party tracking: User exposure to tracking cookies through search. *2013 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technologies*, 1, 549-556. doi: 10.1109/WI-IAT.2013.77

- Graber, M., D'Alessandro, D., & Johnson-West, J. (2002). Reading level of privacy policies on Internet health web sites. *Journal of Family Practice*, 51(7), 642-645.
- Gramm-Leach-Bliley Act of 1999, Pub. L. 106-102, 113 Stat. 1338. (1999).
- Grauer, Y. (2015, October 7). Mr. Robot uses ProtonMail but isn't fully secure. *Wired*. Retrieved from <http://www.wired.com/2015/10/mr-robot-uses-protonmail-still-isnt-fully-secure/>
- Gray, D. & Citron, D. (2013). The right to quantitative privacy. *Minnesota Law Review*, 98(1), 62-144.
- Greenberg, A. (2015, October 29). Tor just launched the easiest app yet for anonymous, encrypted IM. *Wired*. Retrieved from <http://www.wired.com/2015/10/tor-just-launched-the-easiest-app-yet-for-anonymous-encrypted-im/>
- Haynes, A. W. (2012). Virtual blinds: Finding online privacy in offline precedents. *Vanderbilt Journal of Entertainment and Technology Law*, 14(3), 603-648.
- Hill, K. (2014, June 30). Facebook added 'research' to user agreement 4 months after emotion manipulation study. *Forbes*. Retrieved from <http://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/#5352384c10c1>
- Hirsch, D. D. (2011). The law and policy of online privacy: Regulation, self-regulation, or co-regulation? *Seattle University Law Review*, 34(2), 439-480.
- Hoang, N.P. & Pishva, D. (2014). Anonymous communication and its importance in social networking. *16th International Conference on Advanced Communication Technology*, 34-39.
- Information Shield (n.d.). United States privacy laws. Retrieved from <http://www.informationshield.com/usprivacylaws.html>
- Infosecurity (2014, July 3). 'NSA-proof' encrypted email service Tutanota launches. Infosecurity Magazine. Retrieved from <http://www.infosecurity-magazine.com/news/nsa-proof-encrypted-email-service-tutanota/>
- Jaeger, J. (2013). California passes first 'do-not-track' disclosure bill. *Compliance Week*, 10(118), 16-64.
- Kelly, E. (2016, February 21). Congress looks to boost email privacy; Increase social media surveillance. *USA Today*. Retrieved from <http://www.usatoday.com/story/news/2016/02/21/congress-looks-boost-email-privacy-increase-social-media-surveillance/80557184/>
- Kemp, R. & Moore, A. (2007). Privacy. *Library Hi Tech*, 25(1), 58-78. doi: 10.1108/07378830710735867

- Kennedy-Lightsey, C. D., Martin, M. M., Thompson, M., Himes, K. L., & Clingerman, B. Z. (2012). Communication privacy management theory: Exploring coordination and ownership between friends. *Communication Quarterly*, 60(5), 665-680. doi: 10.1080/01463373.2012.725004
- Levin, A. & Abril, P. S. (2009). Two notions of privacy online. *Vanderbilt Journal of Entertainment & Technology Law*, 11(4), 1001-1051.
- Lewis, S. D., Colvard, R. G., & Adams, N. C. (2008). A comparison of the readability of privacy statements of banks, credit counseling companies, and check cashing companies. *Journal of Organizational Culture, Communication & Conflict*, 12(2), 87-93.
- Li, N. (2010). Research on the Diffie-Hellman key exchange protocol. *2010 2<sup>nd</sup> Annual International Conference on Computer Engineering and Technology*, 4, 634-637. doi: 10.1109/ICCET.2010.5485276
- LinkedIn (2014, October 23). Your privacy matters. Retrieved 30 March, 2015 from <https://www.linkedin.com/legal/privacy-policy?trk=uno-reg-guest-home-privacy-policy>
- Literacy Project Foundation (2007) Staggering illiteracy statistics. Retrieved from <http://literacyprojectfoundation.org/community/statistics/>
- Lofgren, Z. (2014). Do modern Americans have fourth amendment protections? *Santa Clara Law Review*, 54(4), 901-929.
- Madden, M. (2014, November 12). *Public perceptions of privacy and security in a post-Snowden era*. Retrieved March 15 2016, from Pew Research Center website <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>
- Malaga, R. (2014). Do web privacy policies still matter? *Academy of Information & Management Sciences Journal*, 17(1), 95-99.
- Martin, A. J. (2016, March 17). Secure email bods ProtonMail open signup floodgates to world+dog. *The Register*. Retrieved from [http://www.theregister.co.uk/2016/03/17/protonmail\\_launches\\_open\\_registrations\\_ahead\\_of\\_snoopers\\_charter/](http://www.theregister.co.uk/2016/03/17/protonmail_launches_open_registrations_ahead_of_snoopers_charter/)
- McCormick, T. H., Ferrell, R., Karr, A. F., & Ryan, P. B. (2014). Big data, big results: Knowledge discovery in output from large scale analytics. *Statistical Analysis and Data Mining*, 7(5), 404-412. doi: 10.1002/sam.11237
- McDonald, A. M. & Cranor, L. F. (2009). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), 543-568.
- Mele20. (2016, March 23). Disturbing [Review of the extension *Ghostery*] Reviews for Ghostery. Retrieved from <https://addons.mozilla.org/en-US/firefox/addon/ghostery/reviews/>

- Meyer, M. (2014, June 30). Everything you need to know about Facebook's controversial emotion experiment. *Wired*. Retrieved from <http://www.wired.com/2014/06/everything-you-need-to-know-about-facebooks-manipulative-experiment/>
- Moore, A. (2008). Defining privacy. *Journal of Social Philosophy*, 39(3), 411-428.
- Moore, S. C. (2012). Digital footprints on the internet. *International Journal of Childbirth Education*, 27(3), 86-91.
- Morio, H. & Buchholz, C. (2009). How anonymous are you online? Examining online social behaviors from a cross-cultural perspective. *AI & Society*, 23(2), 297-307.
- Ohana, D. J. & Shashidhar, N. (2013). Do private browsers and portable web browsers leave incriminating evidence? *2013 IEEE Security and Privacy Workshops*, 135-142. doi: 10.1109/SPW.2013.18
- Papacharissi, Z. & Fernback, J. (2005). Online privacy and consumer protection. *Journal of Broadcasting & Electronic Media*, 49(3), 259-281.
- Peralta, E. (2013, February 26). In discussion about internet privacy, it comes down to expectation versus reality. *NPR*. Retrieved from <http://www.npr.org/sections/thetwo-way/2013/02/25/172909918/in-discussion-about-internet-privacy-it-comes-down-to-expectation-versus-reality>
- Petronio, S. (2004). Road to developing communication privacy management theory: A work in progress, please stand by. *The Journal of Family Communication*, 4(3&4), 193-207. Retrieved from EBSCOhost.
- Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review*, 2(3), 175-196. doi: 10.1111/j.1756-2589.2010.00052.x
- Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication*, 13, 6-14. doi: 10.1080/15267431.2013.743426
- Pew Research Center (2013, November 14). *Internet user demographics*. Retrieved March 15, 2016 from Pew Research Center website <http://www.pewinternet.org/data-trend/internet-use/latest-stats/>
- Pew Research Center (2014, January 2). *Internet use over time*. Retrieved March 15, 2016 from Pew Research Center website <http://www.pewinternet.org/data-trend/internet-use/internet-use-over-time/>
- Pidgin (n.d.) Retrieved from <https://pidgin.im/>
- Preibusch, S. (2015, May 1). Privacy behaviors after Snowden. *Communications of the ACM*, 58(5), 48-55. doi: 10.1145/2663341

- Privacy Act of 1974, Pub. L. 93-579, 88 Stat. 1896. (1974).
- Privacy Protection Act of 1980, 42 U.S.C. § 2000aa et seq. (1980).
- Pollach, I. (2007). What's wrong with online privacy policies? *Communications of the ACM*, 50(9), 103-108.
- Prabhu, V. (2016, February 1). Here are the best 12 email services which will provide you anonymity and privacy. TechWorm. Retrieved from <http://www.techworm.net/2016/02/here-are-the-12-best-email-services-which-will-provide-you-anonymity-and-privacy.html>
- Rainie, L. & Duggen, M. (2016). *Privacy and information sharing*. Retrieved from Pew Research Center website <http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/>
- Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013, September 5). *Anonymity privacy and security online*. Retrieved from Pew Research Center website <http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>
- Right to Financial Privacy Act of 1978, Pub L. No. 95-630, 92 Stat. 3697, (1978).
- Risen, T. (2015, August 25). The illusion of online privacy. *The US News & World Report*. Retrieved from <http://www.usnews.com/news/articles/2015/08/25/the-illusion-of-online-privacy>
- Ruiz-Martinez, A. (2012). A survey on solutions and main free tools for privacy enhancing web communications. *Journal of Network and Computer Applications*, 35(5), 1473-1492.
- Russom, M. B., Sloan, R. H., & Warner, R. (2011). Legal concepts meet technology: A 50 state survey of privacy laws. *Proceedings of the 2011 Workshop on Governance of Technology, Information, and Policies*, 29-37. doi: 10.1145/2076496.2076500
- Seignani, S. (2013). The commodification of privacy on the Internet. *Science and Public Policy*, 40, 733-739. doi: 10.1093/scipol/sct082
- Shmatikov, V. (2011). Anonymity is not privacy. *Communications of the ACM*, 54(12), 132.
- Sidbury, B. F. (2001). You've got mail...and your boss knows it: Rethinking the scope of the electronic communications privacy act. *Journal of Internet Law*, 5(1), 16-22.
- Singer, N. (2016, February 29). Federal efforts in data privacy move slowly. *The New York Times*. Retrieved from LexisNexis Academic.
- Soto, L. J. & Simpson, A. P. (2014). United States in Rosmery P. Jay (Ed.) *Data protection & privacy in 26 jurisdictions worldwide*. Law and Business Research: London, UK.

- Stedman, R., Yoshida, K., & Goldberg, I. (2008). A user study of off-the-record messaging. *Proceedings of the 4<sup>th</sup> Symposium on Usable Privacy and Security*, 95-104. doi: 10.1145/1408664.1408678
- Steinfeld, N. (2016). "I agree to terms and conditions": (How) do users read privacy policies online? An eye tracking experiment. *Computers in Human Behavior*, 55, 992-1000. doi: 10.1016/j.chb.2015.09.038
- Steve, H. (2013, June 23). Keeping track of your digital footprints. *Weekend Edition Sunday (NPR)*. Retrieved March 17 2016, from Ebscohost.
- Strauß, S. & Nentwich, M. (2013). Social network sites, privacy, and the blurring boundary between public and private spaces. *Science & Public Policy*, 40(6), 724-732.
- sukhbir (2015, October 29). Tor Messenger beta: Chat over Tor easily. Retrieved from <https://blog.torproject.org/blog/tor-messenger-beta-chat-over-tor-easily>
- Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat. 56. (1996).
- The White House (2012, February). Consumer data in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. Retrieved from <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>
- Thielman, S. (2015, November 5). ProtonMail: Encrypted email provider held ransom by hackers. *The Guardian*. Retrieved from <http://www.theguardian.com/technology/2015/nov/05/protonmail-service-held-ransom-by-hackers>
- Toxen, B. (2014). The NSA and Snowden: Securing the all-seeing eye. *Communications of the ACM*, 57(5), 44-51.
- Trabsky, M., Thomas, J., & Richardson, M. (2013). The faulty door of cyberspace and implications for privacy law. *Law in Context*, 29(1), 13-25.
- Twitter (2016, January 27) Twitter privacy policy. Retrieved 30 March 2016 from <https://twitter.com/privacy?lang=en>
- USA PATRIOT Act, Pub. L. 107-56, (2001).
- Venkatesh, V. & Brown, S. (2001). A longitudinal investigation of personal computers in homes: Adoption determinants and emerging challenges. *MIS Quarterly*, 25(1), 71-103.
- Video Privacy Protection Act of 1988, 18 U.S. C. § 2710 (1988).
- Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media*, 56(4), 451-470. doi: 10.1080/08838151.2012.732140

- Vranica, S. & Stewart, C. S. (2013, September 20). Advertisers worry about changes in web cookies. *Wall Street Journal*. Retrieved from Proquest.
- Weaver, S. D. & Gahegan, M. (2007). Constructing, visualizing, and analyzing a digital footprint. *Geographical Review*, 97(3), 324-350.
- White, P. & Breckenridge, R. S. (2014). Trade-offs, limitations, and promises of big data in social science research. *Review of Policy Research*, 31(4), 331-338. doi: 10.1111/ropr.12078
- Winkler, S. & Zeadally, S. (2015). An analysis of tools for online anonymity. *International Journal of Pervasive Computing and Communication*, 11(4), 436-453.
- Yue, C., Xie, M., & Wang, H. (2007). Automatic cookie usage setting with CookiePicker. *37<sup>th</sup> Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 460-470. doi: 10.1109/DSN.2007.21
- Yue, F., Wang, G., & Liu, Q. (2010). A secure self-destructing scheme for electronic data. *2010 IEEE/IFIP 8<sup>th</sup> International Conference on Embedded and Ubiquitous Computing*, 651-658. doi: 10.1109/EUC.2010.104
- Zeng, L., Shi, Z., Xu, S., & Feng, D. (2010). SafeVanish: An improved data self-destruction for protecting data privacy. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 521-528.
- Zhao, B. & Liu, P. (2015). Private browsing mode not really that private: Dealing with privacy breaches caused by browser extensions. *2015 45<sup>th</sup> Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 184-195. doi: 10.1109/DSN.2015.18

## **Stephanie D. Winkler**

### **Education**

M.A. University of Kentucky, Communication May 2016 (expected)

B.S. University of Kentucky, Communication December 2013

### **Professional Experience**

Research Assistant, University of Kentucky Summer 2013-Fall 2014

### **Honors and Awards**

Dean's List, University of Kentucky Fall 2013

Dean's List, University of Kentucky 2012-2013

Pi Kappa Delta  
Excellent in Persuasive Speaking 2013

### **Refereed Journals & Magazines**

S. Winkler and S. Zeadally, "An Analysis of Tools for Online Anonymity", International Journal of Pervasive Computing and Communications, Vol. 11, No. 4, 2015.

S. Winkler and S. Zeadally, "Privacy Policy Analysis of Popular Web Platforms", IEEE Technology & Society Magazine, Vol. 35, No. 2, 2016