SOCIAL MEDIA AND ITS EFFECT ON PRIVACY

by

Brittney L. Adams

A thesis submitted in partial fulfillment of the requirements
for the Honors in the Major Program in English
in the College of Arts and Humanities
and in The Burnett Honors College
at the University of Central Florida
Orlando, Florida

Summer Term 2012

Thesis Chair: Dr. Madelyn Flammia

ABSTRACT

While research has been conducted on social media, few comparisons have been made in regards to the privacy issues that exist within the most common social media networks, such as Facebook, Google Plus, and Twitter. Most research has concentrated on technical issues with the networks and on the effects of social media in fields such as medicine, law, and science. Although the effects on these fields are beneficial to the people related to them, few studies have shown how everyday users are affected by the use of social media. Social media networks affect the privacy of users because the networks control what happens to user contact information, posts, and other delicate disclosures that users make on those networks. Social media networks also have the ability to sync with phone and tablet applications. Because the use of these applications requires additional contact information from users, social media networks are entrusted with keeping user information secure. This paper analyzes newspaper articles, magazine articles, and research papers pertaining to social media to determine what effects social media has on the user's privacy and how much trust should be placed in social media networks such as Facebook. It provides a comprehensive view of the most used social media networks in 2012 and offers methods and suggestions for users to help protect themselves against privacy invasion.

DEDICATION

For my mother, Dottie Adams, for reminding me how much privacy matters and that I should never take it for granted. You are my inspiration for this thesis and without your advice and love my ideas never would have taken form.

For my father, Gordon Adams, if they can read theses in heaven, I hope you are proud of what I accomplished. You are not only my dad, but my hero.

ACKNOWLEDGMENTS

I first want to thank my thesis chair, Dr. Madelyn Flammia, for believing in me and encouraging me to persevere throughout this process. Your guidance and insight are invaluable. I also want to thank Dr. JD Applen for fueling my passion for technical communication and leadership. You are more than just a professor, but a dedicated teacher and constant reminder why I chose this profession. To Dr. Malala, thank you for your suggestions and input regarding technology and social media. Your expertise helped in the proposal process and remained useful throughout this writing. I thank you all for serving on my committee and allowing this to be possible. To Bethany Bowles, thank you for your feedback and for increasing my confidence during this process. You are a role model for all students and aspiring technical editors. I could not have done this without your afternoon chat sessions, guidance, and pep-talks. To Michael Cooke, thank you for believing in me. Your endless support and love has gotten me through the toughest of times. To all of my friends and teachers, you made my journey at the University of Central Florida the best time of my life.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER I: INTRODUCTION

The use of social media has skyrocketed within the past ten years. Social media networks, such as Facebook, have allowed people all over the world to connect with friends, professionals, and strangers in a way that was previously nonexistent. The introduction of social media sites has changed the way that people present information about themselves. There are people who use social media to promote businesses, there are people who only have a social media profile for networking, and there are those who use these profiles daily to update others about their lives. Because social media use is frequent, it is worth questioning if users are letting go of some privacy rights. Users are becoming more willing to trust social networks with personal information, such as location, without inquiring about what happens to the information after is it collected by the networks. When users make personal content private on social networks, it is expected to only be accessed by those users. The lack of knowledge about who can access user information on these networks suggests that user privacy may be in jeopardy. According to a *USA TODAY*/Gallup Poll conducted in October 2011, "Only 26% of respondents who use Facebook at least daily said they were 'very concerned' about privacy, compared with 35% who use the social network at least once a week, and 39% who use Facebook less often" (Acohido).

This conclusion has been a common finding in polls regarding privacy on social networking sites. In a 2010 *VentureBeat* article, Sid Yadav discussed a survey conducted by Forrester Research that showed members of older generations, such as Seniors, Older Boomers

(ages 54-64), and Younger Boomers (ages 45-54) were much more concerned about their privacy on these sites than members of younger generations. They found that 50% of Older Boomers were concerned about the issue, versus only 30% of Generation Y (ages 18-29) (Yadav). This data is represented in a bar graph for better understanding in Figure 1.

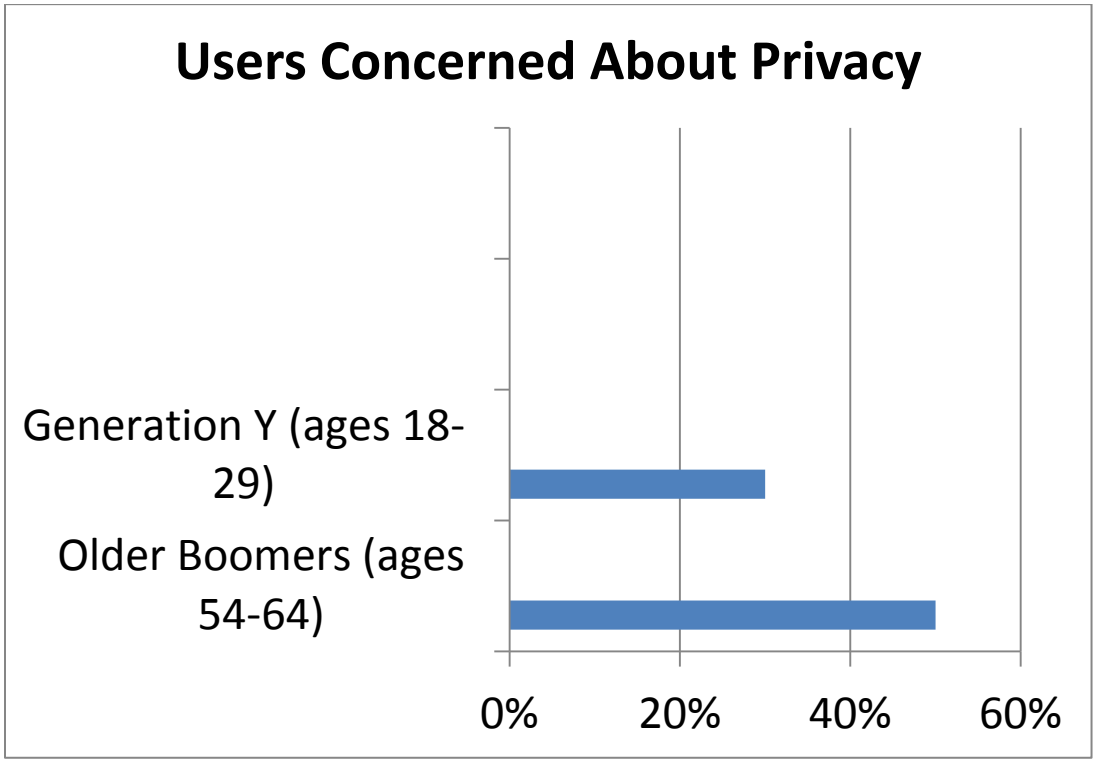

Figure 1: Users Concerned About Privacy

The fact that younger Online Social Network (OSN) users are less concerned about their privacy suggests that privacy is strongly linked to user perspective. Perspectives are clearly different between generations; yet, the reasoning behind these differences is open for discussion. A study by Brandtzaeg, Luders, and Skjetne recognizes these differences by stating,

"This social control often forces younger people in particular to use conformity as a strategy when sharing content…." (Brandtzaeg, Luders, and Skjetne 1006). This study suggests that an increase in Facebook friends leads to a decrease in social privacy, suggesting that younger users tend to feel obligated to conform to the actions of others. Perhaps the younger users value the opinion of their friends more than they value their privacy. It is likely that conformity is the underlying reason why younger generations are paying less attention to their privacy. For example, when one user creates a profile and makes all posts public, the same user's friend may feel obligated or pressured to make his or her posts public as well. Conforming to the expectations of others is a dangerous path for all OSN users. All users, regardless of age, should learn to research the difference between multiple social networks and make decisions that best secure user privacy.

While younger users may be more apt to conform to the acts of other users, younger generation users do have one advantage over other generations of users. When compared with older Facebook users, younger users are "more skilled in their Facebook usage, whereas adults over the age of 40 have difficulties in understanding the navigation logic and privacy settings" (Brandtzaeg, Luders, and Skjetne 1006). The idea that younger users are more familiar with Facebook but less concerned about privacy is surprising considering younger users have the knowledge necessary to change their privacy settings. Younger users likely have more experience with OSN sites and are able to navigate sites easier due to past experiences with similar technology, but neglect to change privacy settings in an effort to conform to other users, such as friends. Because it is evident that younger generations of users are more familiar with

the privacy settings themselves, the Brandtzaeg, Luders, and Skjetne study suggests that older Facebook users struggle with the knowledge needed to protect user privacy, while younger Facebook users simply choose not to change their privacy settings.

Clearly the age of OSN users has an impact on the methods adopted to protect user privacy. Due to the differences in perspective and ability, the importance of all users becoming more aware of privacy issues and methods of privacy protection grows. Younger users need to become more aware of the privacy issues social networks create and older users need to learn about and use the privacy settings that social networks provide. Amanda Lenhart confirms the impact OSNs have on users of all ages in her study which found, “93% of teens and 87% of adult social media users have a profile or account on Facebook…” (Lenhart, et.al). While differences are present between generations, the percentage of overall use is quite similar. This finding furthers the importance that users of all ages learn how to effectively control their privacy settings.

In a recent blog post, Danah Boyd, a researcher at Microsoft, speaking about the methods of controlling who can view a person’s Facebook profile said, “In many ways, deactivation is a way of not letting the digital body stick around when the person is not present” (Sutter). The term "digital body" is striking. A digital body can be considered as any of the information a user displays online that says something personal. The information present in a digital body varies greatly; however, it often ranges from one’s email address and picture, to online biographies or resumes. On social media outlets like Facebook, photos, status updates,

and maps are displayed to create an Internet personality. A digital body on the Internet is similar to a face-to-face introduction. Although users cannot interact physically, the digital body allows people to see other user's pictures, interests, and to view the user's daily life through status updates. Nearly everyone with Internet access has a digital body, and it is likely that most people are also unaware of its significance. By understanding that digital bodies do exist, users can become more responsible about the content they post and how they use OSNs such as Facebook. Users can begin examining how they can improve the privacy of OSN profiles and learn research before making decisions that may affect the user's digital body.

People often want to protect themselves face-to-face, such as making sure debit cards and forms of identification are secure; therefore, it is safe to assume that most OSN users want to protect their digital bodies, or profiles. There are many factors that influence how users can protect their information on social media sites. User awareness is one of the most important factors because unless users are aware of the privacy risks associated with OSNs, no progress can be made in protecting their information. Users must understand the flaws that OSNs have in terms of privacy and disclosing information, and then take the necessary steps to protect their privacy. Users should research other networks that they are unfamiliar with, in case one network decides to include features that a competing network uses. By understanding the risks and having a well-rounded knowledge of the most popular OSNs, users modify privacy settings depending on the amount of information they are willing to disclose to the public and the OSN itself.

Rather than conducting new surveys and quantitative data that many researchers have already completed, this thesis examines the research and information all OSN users should understand. The research analyzed provides users with an overview of Facebook, Google Plus, and Twitter. The privacy policies of all three OSNs are discussed so that users can better understand what areas of the OSN present risks to user privacy. Reading the privacy policies benefits those that may not have an activated social media account, and those that may think they are already knowledgeable on the matter. In addition the research and events that are analyzed, this thesis outlines some methods that OSN users can apply to increase their privacy on OSNs, and encourages awareness. For, the only way to fully protect user privacy is for the user to take responsibility and become educated on the issues OSNs create.

CHAPTER II: FACEBOOK AND OTHER SOCIAL MEDIA NETWORKS

The growth of social media sites has risen at a pace that allows few means for protecting users' privacy. Social media sites offer many different services and along with those services come differences in privacy settings and controls. Before these user controls are discussed, it is important that some social media sites be introduced and that the privacy issues which require change be addressed. Because Facebook, Twitter, and Google Plus are among the most popular social media sites in 2012, analyzing the differences among the OSNs is crucial to determining where privacy issues exist. This chapter discusses the differences in each site's features and privacy policies, so users are better able to determine if and where the information they provide these networks may be in jeopardy.

Introduction to Social Media Networks and Their Privacy Policies

A strong emphasis is placed on Facebook and Facebook's privacy policies in this section because Facebook is one of the most controversial social media networks and its policies are being discussed more frequently as social media networks continue to grow. The specifics of these controversies are described with concentration on the fact that Facebook has gotten several lawsuits and complaints both from users and the FTC urging the network to make changes. This section outlines Facebook, Google Plus, and Twitter and compares the positive and negative aspects of each network and pertinent sections of their privacy policies. A well-rounded view of social media networks and their policies allows users of many networks to

understand what areas present risks to user privacy and what has been done to decrease that risk.

Facebook

At the end of March 2012, Facebook counted “900 million monthly active users” of the site (“Facebook Data Use Policy”). Of these 900 million, “398 million users were active with Facebook on at least six out of the last seven days” (“Facebook Data Use Policy”). The use of Facebook on a daily basis suggests that users place trust in the site. When users trust a network, this trust innately increases the types of data and sensitive information users share to the network. In a comparative study by Dwyer, “Facebook subjects disclosed significantly more identifying information such as real name, email address, and so forth, compared to Myspace” (Dwyer, et. al 6). It is worth noting that Myspace is a site that helped ignite the popularity of social media. At the time of this writing, Myspace still has a noteworthy number of members; however, its popularity has been decreased due to the rise of Facebook and other competing social media sites such as Twitter and Google Plus. Although Myspace has had a decrease in the number of members, Facebook, Google Plus, and Twitter have all seen an increase in the number of members and social media has continued to become a significant part of many people’s lives. Because users have a tendency to trust social media networks to some extent, they create a privacy risk for themselves when exposing personal information. The ideas that users are disclosing personal information leads to the question, what information are users entrusting to Facebook?

Facebook allows users to share pictures, status updates, GPS locations, birth dates, and many other revealing bits of personal information. While the intent of sharing this information is to connect with friends online, many users fail to question whether their information is being misused. User information can be misused when personal information is leaked to other users or applications. These types of leaks are not uncommon and have a significant impact on user privacy. This privacy issue is furthered when users neglect to read privacy policies about how user information is secured, because privacy policies often state how user information is used or distributed.

Ulrike Hugl discussed research conducted by Lawler and Molluzo regarding Online Social Networks (OSNs) which found "that more than half of respondents (US students) did not read the privacy policies statements of their OSNs and about two-thirds did not know how their personal information might be gathered, used, and shared by their OSN providers" (Hugl 392). While US students are not representative of all users, this study does provide some insight as to how many people read privacy policies. If it is assumed that more than 50% of users fail to take the time to review the privacy policies, it is likely that many users fail to adopt personal privacy settings as well. Therefore, users are trusting OSN's to properly handle their personal information, without knowing or considering what is done with it.

Facebook's Privacy Policy

Facebook's privacy policy, last revised on June 8th, 2012, states "Your trust is important to us, which is why we don't share information we receive about you unless we have: received

your permission; given you notice, such as by telling you in this policy; or removed your name or any other personally identifying information from it" ("Facebook Data Use Policy") A large portion of the privacy policy covers how Facebook uses data, such as user information, to improve its features and to give users better advertisements. Facebook's policy states "when we receive data about you from our advertising partners or customers, we keep the data for 180 days. After that, we combine data with other people's data in a way that is no longer associated with you" ("Facebook Data Use Policy"). While this reassurance puts the user at ease to some degree, the policy does not provide specifics on how the information is used other than generally stating that it improves Facebook's features.

Another area of Facebook's privacy policy that causes concern is what happens with users' deleted content, such as pictures, posts, and messages. While their privacy policy fails to cover this area, Facebook addresses it in their Help Center section of the site. The site states that "Some of this information is permanently deleted from our servers; however, some things can only be deleted when you permanently delete your account" ("Facebook Help Center"). Facebook then provides only a hypothetical example, saying, "For example, we save information about friend requests you reject so that we know not to surface those as a people you might want to connect with. We also save information about the tags you remove to make sure that you aren't re-tagged in the same photo" ("Facebook Help Center"). The fact that this policy is not mentioned in more detail in Facebook's privacy policies casts doubt on Facebook's integrity and trust. Understanding what is done with deleted content and why some of it kept is crucial to a trusting user-network relationship. Despite the trust users grant Facebook, the lack

of details about the user content kept and ambiguity of the privacy policy suggests that Facebook does little in terms of reassuring users that their information is secure.

Google Plus

In 2011, Google introduced its own social media site as an alternative to Facebook, Google Plus. While similar to Facebook in terms of sharing photos, posts, and adding friends, it remains unique and has additional features. In addition to basic OSN features such as posts and messaging, Google Plus allows users to create and share documents, connect with different circles of friends, and "tailor [their] search results—based on the interests [they've] expressed in Google Plus, Gmail, and YouTube" ("Google Policies and Principles"). Because Google owns the video outlet YouTube, and offers many other services, Google Plus is able to connect with these features, increasing the amount of sharing and connections users can have. While the integration of these different services provides users with a richer experience, these activities allow more privacy issues to arise. The additional features that Google Plus offers causes users to be more responsible for the information they provide to each Google service. The number of features and integration of services Google Plus provides is what most differentiates this OSN from Facebook. Because many Google services are integrated into Google Plus, Google must ensure that users do not question the security of the OSN and continue to use many of its services. They achieve this by being open about changes made to privacy policies and by addressing the public directly. Successful communication allows the OSN and user to have a trusting relationship.

There is strong evidence that Google strives to earn and maintain their user's trust. In 2012, Larry Page, Google's CEO stated "Users place a lot of trust in Google when they store data, like emails and documents, on our systems. And we need to be responsible stewards of that information" (Page). He also commented briefly on Google's new privacy policy stating that "The recent changes we made to our privacy policies generated a lot of interest. But they will enable us to create a much better, more intuitive experience across Google—our key focus for the year" (Page). Users trust Google because it is the leading search engine; therefore, it is easy to assume that users would trust their OSN as well. The problem with Google's popularity is the same issue present with Facebook; the privacy policies are often complex. Users are not likely to read the privacy policies and to understand fully what is done with their information. Since Google is used for more than just Google Plus, its privacy policy is much longer and covers more areas than Facebook's privacy policy.

Google Plus also has the ability to link Google searches with the OSN, exposing additional personal information. For example, if a Google Plus user searches for a friend's name on the search engine, Google outputs the searched friend's Google Plus profile as a result. This example remains true even if that user's profile is set to private, meaning the public cannot access it. The ability to conduct a search on Google and see connections from the Google Plus account could be useful for some users who wish to access the profile quickly. However, it leaves some users worried that their information is visible from other profiles as well. Although Google has reassured users that only their connections can be seen in the search, the risk of privacy invasion is still present.

In 2008, Bernhard Debatin found "In a report on 23 Internet service companies, the watchdog organization Privacy International charged Facebook with severe privacy flaws and put it in the second lowest category for 'substantial and comprehensive privacy threats'. Only Google scored worse…" (Debatin 84). The study Debatin discussed was completed before the creation of Google Plus. However, these findings lead one to question the privacy flaws present now that Google has expanded. If Google's privacy issues were a concern in 2008, what are they like in 2012 now that many more features have been added?

In January 2012, Google announced that it was placing the majority of its services under one unified privacy policy. Haley Tsukayama clarifies this by stating "Any user with a Google account—used to sign in to services such as Gmail, YouTube and personalized search—must agree to the policy" (Tsukayama). While it is logical that Google would want a unified privacy policy, it leaves users with no opt-out possibility. This means, that in order to have a Google account and to use any of Google's personalized features, the user must agree to Google's overall privacy policy. There is no way to decline certain portions of Google's privacy policy. Even if one service is used and not another, the services are still connected to the user's Google account. For example, in order to use Gmail, Google's email service, you must also agree to the privacy policies for Google Plus even if you do not use the service. While a user may never make a Google Plus profile, the service is still attached to her account through the new privacy policy. The complex nature of Google's privacy policy further signifies the value behind reading privacy policies. It is unlikely that users took the time to read the policy, and this leaves those users open to potential privacy issues.

Twitter

Twitter differs slightly from Facebook and Google Plus as a social media outlet due to its less complex features. Twitter does not offer many applications and limits users to the amount of content they can share at one time. According to Twitter's privacy policy, "Any registered user can send a Tweet, which is a message of 140 characters or less that is public by default and can include other content like photos, videos, and links to other websites" ("Twitter Privacy Policy"). However, Twitter does offer some privacy settings that allow users to make their Tweets more private. In addition to having control over Tweet audiences, users can also control what information is needed for fellow users to find their profile, such as their email address or full name.

A PEW Research Center study found "Some 15% of online adults use Twitter as of February 2012, and 8% do so on a typical day" (Smith and Brenner 2). Yet, adults are not the primary users of Twitter. The same study found that "one quarter (26%) of internet users ages 18-29 use Twitter" and "among the youngest internet users (those ages 18-24), fully 31% are Twitter users" (Smith and Brenner 3). Because there are twice as many younger users as adult users, one could question whether the younger users are as aware of the privacy risks they accept when using the OSN. Unless they read the privacy policy or research the privacy issues thoroughly, users cannot develop a solid understanding of what OSNs such as Twitter do with user information. If users are not reading the privacy policies, are they being conscientious about the content they display to the public or provide the OSN? Amanda Lenhart was among a

group of researchers that found “More than half of online teens have decided not to post something online because they were concerned it might reflect badly on them in the future” (Lenhart, et. al.). United States citizens are fortunate to have certain rights such as the freedom of speech, but the unknown actions of OSNs like Twitter—such as what they do with user content—may cause many American users to retract this right by choice. For example, a user may want to make a Twitter post that comments on the economy, but refrains from posting because he is afraid of possible consequences such as his boss disagreeing with his opinion. While not all countries in the world have the freedom of speech, it is likely that many international users want to be able to state their opinions freely on Facebook as well. If users around the globe are not speaking their minds on Twitter as they would in a conversation, it suggests that the user and OSN relationship is not as trusting as it could be. The fear of potential repercussions from posting certain information or thoughts on an OSN suggests that not all users are willing to blindly trust the networks.

Similar to Facebook and Google Plus, Twitter’s settings are general with no additional privacy tools that would make Twitter stand out from the others in terms of privacy risk. In fact, Twitter notes in its privacy policy that user information is largely distributed and that “public user profile information and public Tweets may be searchable by search engines and are immediately delivered via SMS and our API’s to a wide range of users and services, with one example being the United States Library of Congress, which archives Tweets for historical purposes” (“Twitter Privacy Policy”). Since Twitter automatically sets default privacy settings to make all user information public, it increases the risk of privacy issues. If users are not reading

the privacy policies, they may be unaware that Twitter makes information more public than some other OSN's. By reading the privacy policies, it is clear that Twitter is much more open about how user content is used.

Because Facebook, Google Plus, and Twitter all have areas where privacy could be improved, it should not be surprising that governments around the world have taken action against these OSNs. Primarily, the actions of Facebook have been the focus. However, the difference in actions between the United States and Europe are significant because users in Europe have become more protected than US users. Governmental actions have varied depending on the country the Facebook accounts reside, many concerning the data that Facebook retains on each user. By analyzing what has been done, users can be more aware of what should be done to protect user privacy in the near future.

Government Involvement

In 2011, the Federal Trade Commission (FTC) filed a complaint against Facebook. The FTC had received several complaints stating Facebook was deceptive, because they failed to inform users about changes to their privacy settings. These deceptions included changes made to Facebook in 2009 that retroactively caused information that users had previously made private to become public without notification. For example, some users posted status updates and pictures that they marked private, but later found that Facebook changed them to a setting that made them public, without the user's consent. This caused anyone to be able to view user pictures and statuses at any time. Such a breach in privacy suggests that Facebook does not

keep their content as secure as many users believe. Breaches in privacy settings directly affect users by displaying their private content.

The breaches in privacy settings are significant because users have an expectation of privacy. This expectation is best shown by analyzing the Fourth Amendment to the Constitution which protects U.S. citizens from unlawful search and seizure. Danah Boyd and Nicole Ellison discuss this concept by stating:

> The Fourth Amendment to the U.S. Constitution and legal decisions concerning privacy are not equipped to address social network sites. For example, do police officers have the right to access content posted to Facebook without a warrant? The legality of this hinges on users' expectation of privacy and whether or not Facebook profiles are considered public or private (Boyd and Ellison).

While police searches of Facebook profiles is an extreme example, users could argue that Facebook accessing user profiles and changing settings may also fall under the Fourth Amendment because they are essentially searching user information and changing the disclosure of content. It has also been noted that "The Constitution does not protect information that one has "knowingly exposed to the public" (Freiwald). Facebook changing content to public after the user made it private suggests that users did not knowingly expose it to the public. While it falls in a gray area and many could argue the Fourth Amendment does not relate to social media searches and seizures, users have an expectation of privacy from social media, and should be concerned that the Constitution does not protect them from

certain types of electronic communication seizures and searches. While the constitution does not currently provide protection, the FTC has provided some requests for user protection.

A settlement was made with the FTC in late 2011 that required Facebook to change some of their protocols. One of these changes demanded by the FTC states that Facebook is now "required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account" (Federal Trade Commission). Although the proposed time limit for information to be deleted is an improvement, the delayed deletion time still presents the risk of someone accessing the material. Just because Facebook must make efforts to prevent it from happening does not mean that the deleted content will never be seen again. Although the change is a step in the right direction, users should be aware that Facebook openly admits to keeping advertising data for 180 days after its initial use. If a user deletes content, OSNs should not be allowed to store the content on their servers. By storing deleted user information, Facebook's actions are not only questionable, but it suggests that Facebook lacks ethical standards. While they may claim that nobody has access to the deleted content, they cannot ensure the public that a breach in privacy will never happen again.

It is disturbing that Facebook took two years before settling with the FTC on privacy changes. Facebook merely settled the case by agreeing to make changes to their policies versus facing stronger consequences such as fines or stricter regulations. Facebook was never charged for breaking federal law for deceiving consumers and failing to keep privacy promises. While it is unknown how Facebook has avoided severe consequences, it could be due to their extensive

lobbying efforts. According to Fredreka Schouten in *USA Today* in 2011, "Facebook spent $910,000 to lobby Congress and federal agencies during the first nine months of the year, more than twice what is spent on lobbying in all of 2010" (Schouten). Breaking federal law and allowing private user content to become exposed are not crimes that should be taken lightly. Facebook has an obligation to users legally, professionally, and ethically. When companies such as Facebook are allowed to settle for changes, it sets a precedent that other social media outlets can do the same.

While Congress is taking limited action to address these particular privacy breaches, the focus has been on the privacy of American workers in connection with their Facebook accounts. In March 2012, House Republicans blocked the Facebook Protection Amendment, which "would have let the Federal Communications Commission prevent employers from forcing workers to reveal their Facebook passwords" (McAuliff). The attempt stemmed from concerns among users that some employers were demanding passwords to employee Facebook accounts so they could view any activity the workers posted. For example, a newly-hired employee could be asked to provide her employer with her password and Facebook profile. If the user does not give the employer the information, the user can face not getting the position or being fired for withholding the information. Because some users value their privacy and do not want to disclose some information and passwords, the decision allowing or preventing employers from requesting user information from employees has been a troubling issue to both users and the government. Yet, the American government has provided no preventative action thus far, and users have been left to either to accept the risks associated with having a Facebook account, or

to delete their accounts. Although privacy rights in America remain in jeopardy, Facebook users in Europe are making progress in protecting their rights.

Max Schrems, a student from Vienna, Austria, requested his Facebook data to determine what information Facebook maintained on his account. As a citizen of the European Union (EU), he had certain rights provided by EU directives. Using the rights granted to him under EU directive 95/45/EC, he had the ability to request and receive all the information that companies such as Facebook maintain on citizens (O'Brien). He later received over 1,200 files that contained information he had previously deleted from his account. He felt that his privacy was in jeopardy and did not think that Facebook should be able to keep information he had deleted. After all, the main purpose of deleting documents is so that others can no longer view them. His discovery that his privacy was endangered led him to form the group Europe vs. Facebook (O'Brien). It is important to note that Facebook Inc. controls all accounts in the United States and Canada. Facebook Ireland Limited controls all the accounts in Europe (Facebook).

Since its formation, the Europe vs. Facebook group has prompted Facebook Ireland Limited to make several changes regarding the information companies can keep. The Office of the Data Protection Commissioner in Ireland released the results of an audit of Facebook's practices regarding privacy. The Commissioner announced that their findings led to minor changes, such as increased privacy controls and limits on how long certain information can be kept in Facebook's computer systems (O'Brien). Plenty of attention is being paid to these issues

in Europe, and changes are being made to Facebook accounts there. Given the changes in Europe, we might expect to see Facebook Inc. make similar changes to American and Canadian accounts because the desire to protect user privacy is a global issue. Since European countries are making more progress protecting user privacy than the United States, it suggests that the same can be done in America if users continue to push for awareness and change.

Facebook should not be allowed to keep all of the information that users delete because users deleted it for a reason. Information that is deleted by the user should remain deleted entirely. When OSNs like Facebook store the deleted information, it sets a precedent that other OSNs can do the same. Not only should consumers be made more aware of these issues and learn what is being done with deleted content, they should also understand the risks that are associated with using OSNs. Users who designate content as private should not trust the OSNs settings implicitly. Although the settings may be set to make posts private, it does not eliminate the possibility of the information being leaked or made public by the OSN in the future. A user is on a slippery slope when she fails to secure content. Because relatively no action has occurred in America to protect user privacy, it is crucial that users learn methods that can increase their privacy on social networks such as Facebook. An improvement in understanding allows users to protect their digital bodies, or profiles, on Facebook in order to achieve optimal privacy when it comes to others viewing their profiles and accessing their content.

CHAPTER III: SOCIAL MEDIA APPLICATIONS

As smartphones, tablets, and other technologies become more portable, OSN's become easier to access and quicker access strengthens the risk of privacy invasion. When smartphone technology grows, so does the amount of information users store on their mobile phones. In addition to contacts, calendar dates, messages, and photos, users can also download games from smartphones using operating systems such as Android. Many games are also downloadable to other personal devices such as computers and tablets. Users who download these features can speed up registration processes, such as log-in time and username creation by syncing them with email addresses or OSN profiles. While social media games may seem like safe items to download on personal devices, many users underestimate the amount of information that the games require in order to be installed on devices. Users who do not read the permissions before downloading the application or who openly provide the application with their personal information are becoming targets for privacy invasion.

Social media games, commonly referred to as applications or apps, often require the capability of creating accounts with Facebook, Twitter, or Google Plus accounts. A *USA Today* article by Byron Acohido states that "Some 10,000 new websites integrate with Facebook every day, and Facebook members alone install some 20 million social media apps every day" (Acohido). While Facebook enabled applications are a convenient feature, the applications also require certain permissions from the user. If the user does not read the privacy policies carefully, he risks accepting privacy policies and permissions that significantly increase the risk

of the user's privacy being violated. This chapter discusses the most common privacy permissions that users accept upon download of these increasingly popular applications, as well as the permission's relation to user privacy.

Android

Android is a mobile platform that "powers millions of phones, tablets, and other devices and brings the power of Google and the web into your hands" ("Discover Android"). For the purpose of this thesis, concentration is placed on Android applications. Applications are downloadable games, content, and other media that users manually select from the Google Play store. This digital store is available on all Android operated devices and provides both free and paid applications. Because limited research exists on the privacy risks and effects of these games, user awareness needs to be increased. When research is conducted and popularized by newspapers and journals, users are more likely to become aware of the risks associated with OSNs. Yet, when research is limited, users are left with relatively no information about these risks. Despite the amount of research available, users can limit privacy risks by reading and understanding the meaning behind the permissions they accept upon downloading these applications.

Before users can download applications, they must first accept permissions created by the application's developer. For example, all applications are available through the Android device, but outside developers create most of the applications. Therefore, the developers, or creators, of the applications access Android's list of permissions and can choose to include any

of them in the application's code. Because the Android software is not responsible for placing permissions in the applications, outside developers can request access to the user's personal information, sometimes with malicious intent. The permissions are placed in the application by using strings of code that ask the user to accept the risks. When users review these permissions, a short description is provided that tells the user why the permission is needed. The developer section of the Android site states "Our convention for the description is two sentences, the first describing the permission, the second warning the user of what bad things can happen if an application is granted the permission" ("Android Developers Guide"). Because the descriptions are short, users do not always receive enough information about the permission to confidently decide whether or not to accept the permission's request. While the application does not hide these permissions and requires users to view them before downloading, there is not enough information provided in the description for user's to have a comprehensive understanding of the permission's effect. User awareness of these permissions is the best way to protect users from privacy risks associated with the applications. This section outlines the most frequent permissions that Android applications request from users, what the permissions allow the application to do, and any associated privacy risks.

Fine Location Permission

According to Android, this "allows an application to access fine (e.g. GPS) location" ("Android Reference"). A GPS location can be needed by applications in order to provide information that is based on the user's location. Such information could include weather,

shopping, directions, and other location-sensitive topics. While allowing an application to find a user's location may seem harmless to some users, it does put the user's privacy at risk. William Enck, Machigar Ongstang, and Patrick McDaniel discuss this risk with an emphasis on the intent of the permissions. Similar to the fine location string, they used FriendTracker which is in application that requires permission to find out if the user's phone is near the one or more of the users' friend's phone locations. It completes this action by using the permission string titled "FRIEND_NEAR" (Enck, et. al). This string is similar to the fine location string because the user's location is required in order for the application to work successfully. While the string is not specific about the method used to find the user's location, it is likely that GPS is the preferred method. The problem with this type of permission is that "it potentially informs all installed applications of the phone's proximity. In this case, sending the unprotected intent is a privacy risk" (Enck, et. al).

Enck, Ongstang and McDaniel further explain the privacy issues with permissions by outlining what steps Android takes to avoid sending this data to other applications. Yet, the responsibility is placed primarily on the application developer. Android "optionally allows the developer to specify a permission label to restrict access to the intent object" ((Enck, et. al). Therefore, the developer has the option of preventing other applications from receiving the user's location data. It is important to emphasize the developer's role in privacy. By downloading a game or application with any location-detecting terms, the user trusts that the developer took the time to secure these permissions. For example, when a user downloads an application, she puts trust in the developer because she expects that the developer is not using

her personal information and content maliciously. The user is trusting that the developer is protecting her content and not allowing other devices or people to access it. Enck, Ongstang, and McDaniel proposed several questions regarding the security of permissions such as FriendFinder stating "Even with all the refinements, holistic security concerns have gone largely unaddressed. First, what does a permission label really mean? The label itself is merely a text string, but its assignment to an application provides access to potentially limitless resources" (Enck, et. al). Specifically, a permission label gives the application permission to conduct a specific act, such as using the device's memory card, but does not set limitations on what happens with the data collected. The user is left unaware of who has access to the information and if it is being used securely. Enck, Ongstang, and McDaniel's research was conducted in 2009, and now in 2012, these questions remain unanswered, increasing the importance that users become more aware of the permissions they accept upon downloading applications.

Audio and Recording Permissions

Many users are also unaware that permissions exist that allow applications to complete a number of unethical acts, such as listening to the user's conversations, calling contacts, and accessing all of the user's contact information. While Android warns that some of these permissions could be used maliciously, no changes have been made to prevent developers from using certain permissions. Eliminating some of the invasive permissions such as the permissions described above would limit what developers could access and include in their applications. Since developers are not being limited in terms of what they can request access to on a user's

phone, these permissions present risks to the user's privacy. Because many of these permissions are accepted without the user having a full understanding of the permission's ability, these permissions are often accepted by the user in hopes that the application can be trusted to not use the information in a way that puts the user's information at risk.

In a recent *PC World* article, Ian Paul and Brent Rose outlined the privacy issues with smartphones with an emphasis on location security and other data collection such as noise. Paul and Rose note that some apps have the ability to turn on a user's "microphone to listen to background noise and report back to their creators what they hear" (14). While this type of permission would be listed before downloading the application on an Android device, it is unlikely that the user would know from the brief description exactly what the permission allows. The permission for this type of activity is listed as "RECORD_AUDIO" when the application requests permission ("Android Reference"). The title of the string is vague and one would generally assume that it means the application has the ability to record audio when the user desires, perhaps for a voice recording application. Android vaguely describes it as "Allows an application to record audio" ("Android Reference"). Similar to the small description of the location string, the record audio string does not give the user enough information before download regarding what this permission allows.

Applications that record and listen to audio are not uncommon. Color and IntoNow are used in Paul and Rose's article as examples of smartphone applications that request permission to record audio. The article states that "By comparing the sound patterns across many phones,

the creators claim, the apps can better determine whether people are in the same room, say, or watching the same program on TV" (Paul and Rose 14). For example, a user could download an application that requires recording audio, have a conversation with a friend, and the application would remember key words that were mentioned in the conversation. The key words that are recognized can be used to achieve a number of tasks, such as providing the user with links related to those key words. The outcome of recording audio from a user's phone directly depends on the application's purpose, leaving room for malicious applications to use the audio in ways the user did not expect.

The ability to listen in on personal conversations is one of the most profound examples of a permission users may not want to accept. Yet, the vague description upon download does not outline that this is the application's intent. It should be noted that not all applications use the record audio string in order to listen to private conversations. Paul and Rose include ShopKick as an additional application example that does not have the intent of listening for specific words stating "The makers at ShopKick, meanwhile, say that their app is for listening for a special tone (inaudible to human ears) so that it knows when you are in a store that offers a ShopKick discount" (14). While the idea of recording inaudible sounds may seem better than recording actual conversations, either use is still likely to surprise users who download the application. Users who read the permission's description may not understand why the application needs the phone's microphone, but assume that it is being used securely. Users have an expectation that when they accept the permission, no negative consequences will occur. As a *Wall Street Journal* article notes, some "Apps are required to ask people's

permission to access their Facebook data. But the way they ask plays on a fundamental human tendency—namely, that people who see frequent warnings come to disregard them" (Angwin and Singer-Vine). Humans are creatures of habit, and when we get used to accepting permissions when downloading apps, the more likely it is that we will do it again. The permission strings need to be more specific in their descriptions so that users can be more educated about what they are allowing an application to access and keep on file.

Other Permissions

Location and audio are not the only permissions that present a danger to user privacy. Guanling Chen and Faruq Rahman point out that other permissions do not provide feedback regarding if "users' other information, such as the identity, phone number, calendar, contact list, and call history, is implicitly collected by these applications" (Chen and Rahman 85). Chen and Rahman also express concern with the fact that some applications are created independently and some can be created anonymously. Because applications can be created by anyone, the user is left to determine if the application has a favorable intent. Although most applications require the user to accept permissions for this information, the verbiage in the permission notice is vague. One of the most significant examples of this is the fact that applications do not state what is done with the information collected. For example, the "READ_CONTACTS" string states that it "Allows an application to read the user's contacts data" ("Android Reference"). The short description of the string does not provide the user with a specific use for the information. The description does not state why the permission is needed or

where the information collected will be used after it is read. The lack of details regarding the permission's intent leaves the user with minimal knowledge about what the permission intends to do. Therefore, a user could grant permission to an independent developer who does not work for a reputable company, or a dependent application developer, who does work for a reputable company, and remain unaware of where the information is being sent, sold, or used.

In addition to recording audio and finding locations, application permissions can request to have access to users' personal contacts and can even request to place outgoing calls on the user's behalf. Paul and Rose referenced a *Wall Street Journal* study that found "that most of the 101 apps it tested shared a phone's unique ID number with third parties" (14). Thus, users who download some applications can be tracked through their phone's ID number and solicited to parties such as advertisers and other developers. Paul and Rose discovered that some applications require permissions including latitude, longitude, contacts, age, gender, and phone number, and that many users are unaware of the data's significance (14). All of this information is significant because it is sensitive information for most users and meant to stay private. While some of the applications in the study do not connect directly to Facebook and other OSN's, they are still considered social due to the ability to connect with other contacts.

The Social Network Connection

Many OSN's connect with applications in an effort to broadly share information across platforms. For example, a user may use a phone application to update a status to Facebook, Twitter, and Google Plus simultaneously. Thus, when a user updates to one site, the others are

updated as well. Chen and Rahman provide an example of this connection stating that "a video marked as favorite on YouTube may get published on FriendFeed, and then pushed further to Facebook" (86). The blend of applications with several OSN's causes many gray areas in terms of privacy. When more services, applications, and OSN's are involved, the more complex and plentiful the privacy policies become. Most applications do not disclose what happens to the data collected; therefore, the user is increasingly responsible for the decisions they make in terms of sharing information. While content sharing applications are convenient for users who frequent multiple OSN's, users need to understand that even by posting statuses, pictures, and other content to their social network directly, their privacy is still in jeopardy. The lack of understanding is particularly true for Twitter because they allow "third parties to retrieve the public timeline, thus a user may never know where her updates eventually reach" (Chen and Rahman 86). Summize is owned by Twitter and "archives Twitter's public timeline messages and makes them globally searchable" (86). Users may choose to place their statuses on Twitter with default privacy settings, and be unaware that their content is available for anyone to see on the Internet. Chen and Rahman take that scenario further by stating "If a user later chooses to delete some of her updates on Twitter, the messages still remain in third-party repository…and are likely to be still publicly available" (86). In addition to inquiring how long Facebook and other OSNs keep user information, users should also question why the third-party application is holding on to data and what it is being used for. Unfortunately, most applications do not disclose this information, leaving users to judge the risk.

Users should choose the applications they download wisely. All users should research the permissions each application requests before accepting the terms. While some applications do use permissions for the user's benefit and do not intend to put user privacy in danger, there are some applications that do use permissions with unethical intent. Distinguishing which applications have good intent and those that do not is up to the user. If an application asks for permissions that the user does not believe are needed for the application's purpose, it may be a signal that the application is using the permissions maliciously. Users need to understand that downloading any application is in some way taking a risk and putting personal privacy in the hands of other individuals, including application developers.

CHAPTER IV: METHODS OF INCREASING PRIVACY

Although the use of social media outlets and applications increases the risk of privacy issues, there are several methods that can be used to decrease these risks. The responsibility remains primarily on the user. Thus, it is important that users educate themselves on the privacy settings that OSN's offer, and how they can use them to their advantage. OSN's do not always make these settings easily accessible to users, therefore, knowing where to search for privacy settings is an integral part of the process. While privacy settings can change frequently, they are generally found in the same sections of the OSN's and do not change drastically enough for the steps below to become outdated. Users should check their privacy settings often so that any new settings can be considered. Even though user settings do not eliminate the risk of privacy invasion, they can protect users from disclosing personal information such as statuses, pictures, and contact information from being displayed to the public.

Facebook Account Settings

When users log-in to Facebook, there is no obvious text on the page that suggests privacy settings can be changed. Because no direct link is given on the main page, users can be led to believe that privacy settings do not exist. Yet, the privacy and account settings features do exist and they are just a few clicks away. Figure 2 shows the top of the main page that is shown when a user logs in.

Figure 2: Main page (Facebook)

On the top right hand side of the main page, there is an arrow next to the "Home" button. While this arrow may seem small and insignificant, it is the most important button that Facebook users can know and refer to often. Figure 3 shows the options listed once this arrow is clicked by the user. Account settings are used to change information such as the user's email address and phone number. General privacy settings are not usually found within the account settings option, but options regarding advertising are located here. Since advertisers can sometimes receive user information, all users should edit their settings through this tab. Because privacy options change often and it some privacy settings such as advertisements are hidden in the account settings tab, it is important that users check this tab frequently for changes and additions.

Figure 3: Dropdown menu (Facebook)

Once users select “Account Settings” from this dropdown menu, a new screen will appear that lists the user’s general information. In the left hand corner, there is a list that has many options to choose from such as “Security,” “Subscribers,” and “Mobile”. Yet, for the purpose of speedy user privacy protection, there are two options that should be emphasized: “Apps” and “Facebook Ads.”

Facebook Ads

At the time of this writing, “Facebook Ads” is a relatively new option that users can select to change their privacy settings regarding current and future updates to the way Facebook presents ads to its users. One of the most important reasons why users should check this section frequently is because of its relevance to future features that Facebook may add. For example, when discussing ads shown by third parties, Facebook states “Facebook does not give third party applications or ad networks the right to user your name or picture in ads. If we allow this in the future, the setting you choose will determine how your information is used” (“Facebook Ads”). Statements that mention prospective options make Facebook appear as though they have considered providing third parties with user information. While it is encouraging that Facebook has options for users who do not want their information by third parties, the options to change settings could easily be overlooked by users. Although “Facebook Ads” is an option in Facebook’s privacy settings, most privacy settings on OSNs do not offer the user opportunities to change settings for future features. Therefore, the average user would not consider “Facebook Ads” as an important setting that protects privacy. The name

“Facebook Ads” could be misconstrued to be a setting that users can select to create an advertisement themselves. However, by selecting the option, users then learn that privacy risks exist in the “Facebook Ads” section of settings as well. Users should make a habit of checking all sections of the privacy settings because just reading the name of the section is not always enough to realize its significance.

In Figure 4, two red circles highlight the options available for users to change their settings regarding advertisements. Users will find that these options are scarce, but do provide users with a choice in how their information is used. The first option “Edit third party ad settings,” allows users to update one setting that prevents third party applications and advertisers from using the user’s name or picture in ads. While this feature is not currently applicable, this setting prevents user information from being used should Facebook change their policy. The user can choose to display her information to “no one” in the dropdown box that appears and then save changes. Once the user completes this update to the privacy settings, the user’s account is now protected from third party advertisers now and in the future.

The second option, “Edit social ads setting,” allows users to opt out of social ads. Social ads are personalized ads that appear when users are on the OSN. Facebook states that “These ads are chosen based on the things you do with Facebook such as liking a page, and info Facebook receives from you and other sources” (“About Facebook Advertising”). Therefore, if the user likes an ad or the ad’s Facebook page, the user’s Facebook friends will see a statement below the ad that tells them their friend liked it. While the user’s information is not sold to the

advertiser for these social ads, other the user's friends are still able to see activity that in some cases may be considered sensitive. Similar to the first "Facebook Ads" setting mentioned, users can choose to display their name to "no one" in the dropdown box. By changing the setting and saving changes, users can prevent Facebook from using their interests and name to promote paid advertisements. These settings can also be accessed through the privacy settings tab.

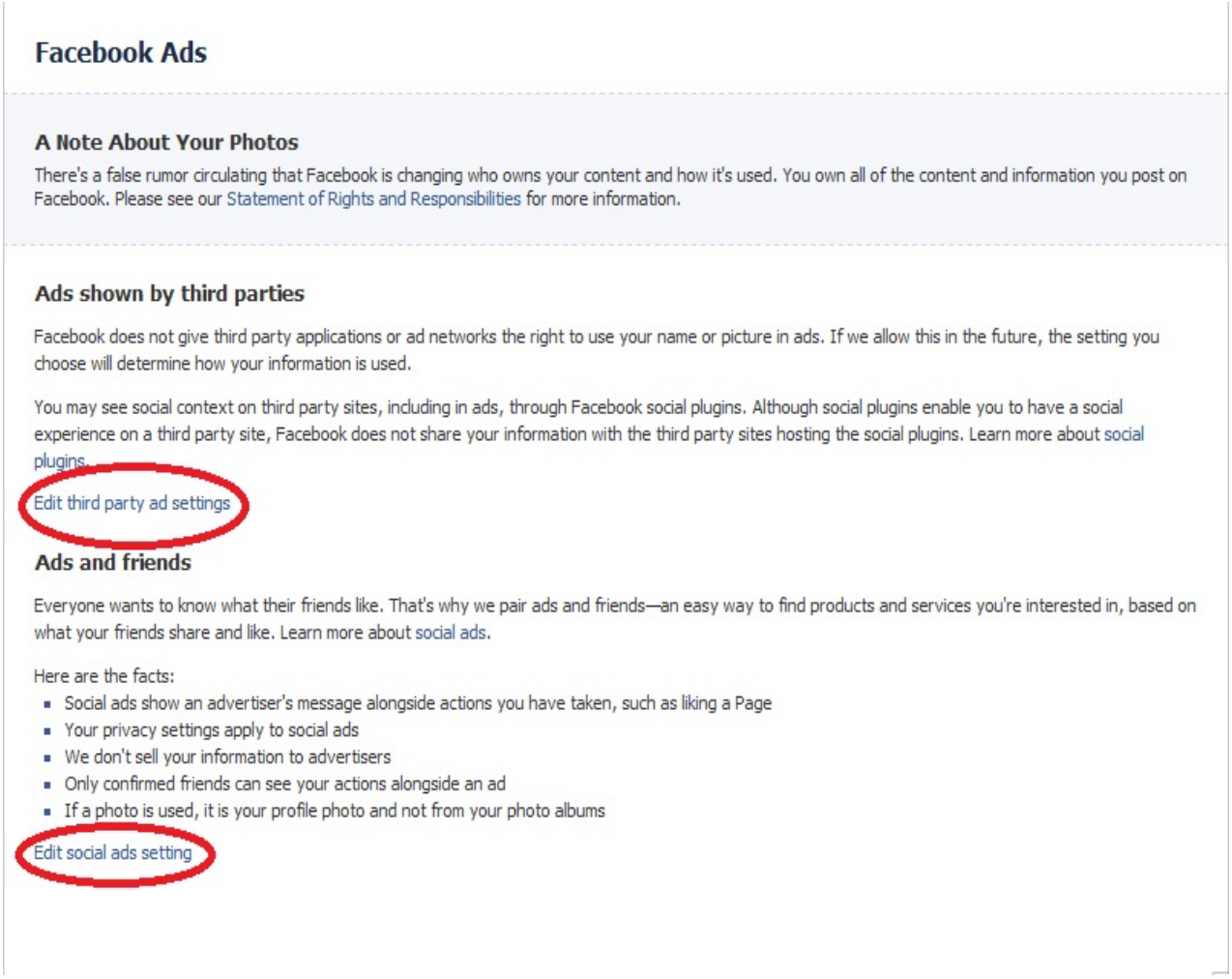

Figure 4: Facebook Ads Privacy Settings (Facebook)

Facebook and Apps

The apps feature of Facebook's "Account Settings" option allows users to view what applications they are currently using or that are still linked to their account. Some of these apps connect with the user's smartphone. For example, if a user downloads an application on her phone, it may have the capability to sync with their Facebook account if given permission. By selecting the apps menu from the "Account Settings" page, users can simply delete applications that have permissions to their Facebook account. Applications can be deleted by pressing the "x" mark next to the application they wish to eliminate. Users should keep in mind that deleting the application from the OSN does not delete the application from their phone; therefore, the user should also uninstall the application from her phone if applicable. For example, if an application was downloaded on the user's phone and synced to his Facebook account, the user should uninstall the application on the phone in addition to deleting it on Facebook. Once the application is deleted on both ends, the application no longer has access to the permissions or terms that the user accepted upon download. Eliminating the use of applications is the best way to prevent them from having access to private information. Users who still want to use applications, either on their phone or on Facebook, should make an effort to read the terms and conditions, as well as the permission descriptions before downloading or using an app. By reading this information, users can stay more informed about what details they are providing the application developer or OSN.

Facebook Privacy Settings

The “Privacy Settings” option from the dropdown menu shown in Figure 3 is the best method that users can adopt to protect their privacy. The “Privacy Settings” page offers several categories that users can choose from to control settings. These categories are always changing so it is important for users to check them often for any additional settings they may need to update. This page allows users to update settings that control what information other users can see, apps can use, audiences for the user’s posts and pictures, as well as who can post on the user’s wall or timeline. All of these features are crucial to protecting a user’s privacy. There is no substitution for going through all of these categories and making sure that privacy settings are as desired. Facebook often defaults privacy settings, so without navigating through this page and manually changing user privacy settings, user’s risk displaying information they want to be private. Facebook does note on the privacy settings page that “the people you share with can always share your information with others, including apps” (“Privacy Settings”) Therefore, users must consider who they designate as the audience of their post. Users can control who views postings by paying close attention to the audience selection when first making a Facebook post. Figure 5 shows a graphic that Facebook uses to show this feature on the “Privacy Settings” page.

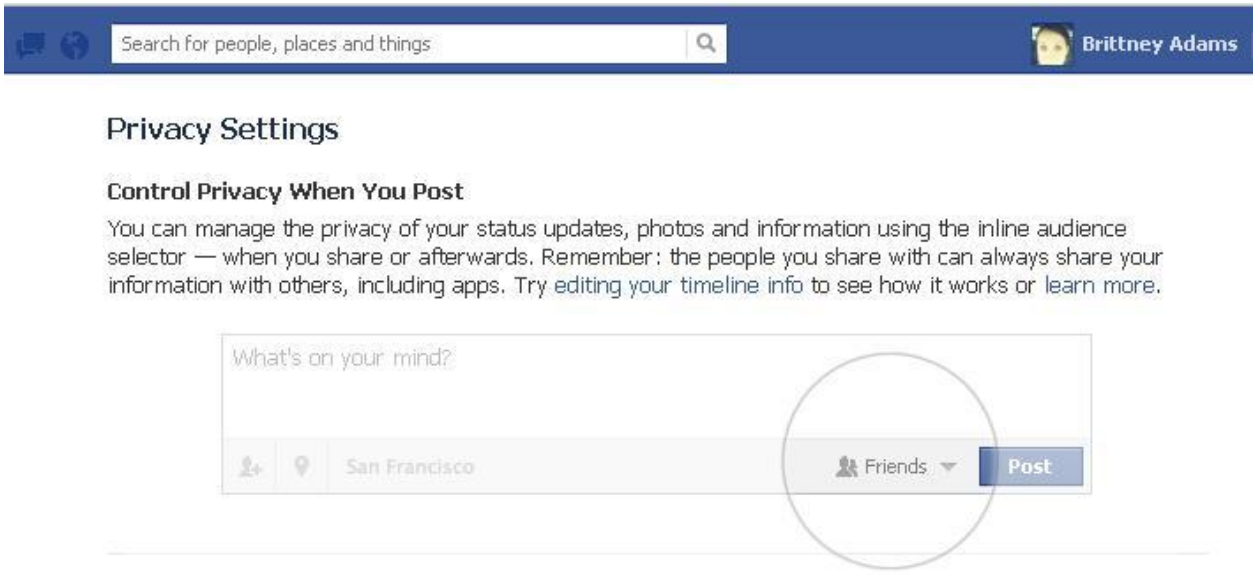

Figure 5: Audience Setting (Facebook)

The circled area shows an icon that can be selected to change the intended audience of the user's post. Because posts can include pictures, links, media, and statuses, this is one of the most efficient tools that users can learn. Users can make posts specifically for groups of people, one person, all friends, or just make the post private for only the user to view. Before posting any content, users should consider if the post is appropriate for all audiences and if they mind the public viewing it. The amount of privacy a user wants is dependent on the settings the user chooses. For example, if a user wanted to make a posting that is not suitable for all audiences, such as users under 18, the user could modify the audience of the post so that the users under 18 could not see the post. This could be done in a number of ways, the most convenient being placing all of the underage users in a group other than "Friends". Specifically, the user could

add the underage friends to a custom list such as “Kids in the Family” so they are not included in the users mass “Friends” list. By selecting the audience dropdown box before posting a status or other content, the user can then choose to show the post to “Friends”. Because “Kids in the Family” users are separate from the friend’s list, they will not be able to view the post.

Deactivation

Users can also choose to deactivate their accounts at any time. Deactivation is the best option for users who do not want their profile accessed at all. Users who deactivate their accounts do not delete them. Simply put, deactivating the account allows Facebook to keep all of the user’s information until the user decides to make his account active again. Deactivation is useful if the user is worried about a potential employer seeing his account, or as a particularly drastic way to protect his privacy. Users with deactivated accounts cannot be searched by the public and their Facebook friends can no longer see their profile and activity. Deactivation can be completed by selecting the “Security” tab on the “Account Settings” page.

Deactivation can be completed on most OSNs and is often an option within the account settings menu. Users who want to deactivate accounts are taking a proactive approach to protecting their privacy. By deactivating his account, the user no longer needs to worry about applications accessing data, or posts and pictures becoming public instead of private. Deactivation is the best method for those users who do not want to lose pictures and content completely. The account can always be reactivated; therefore, users can retrieve data that they may want to save or have access to at a later date.

Google Plus Settings

Google Plus and Twitter have different settings that users can choose to improve the privacy of their profiles. Google Plus has a much more organized method to updating settings. By simply selecting the button with a picture of a gear on it at the top of the user's profile (shown in Figure 6), the user is directed to another page that lists all of the elements needed to update privacy settings. This button is large enough that most users should find it with ease. However, because the button does not say "settings" until the gear button is selected, some users may not know by first glance that the gear button is where the settings are located.

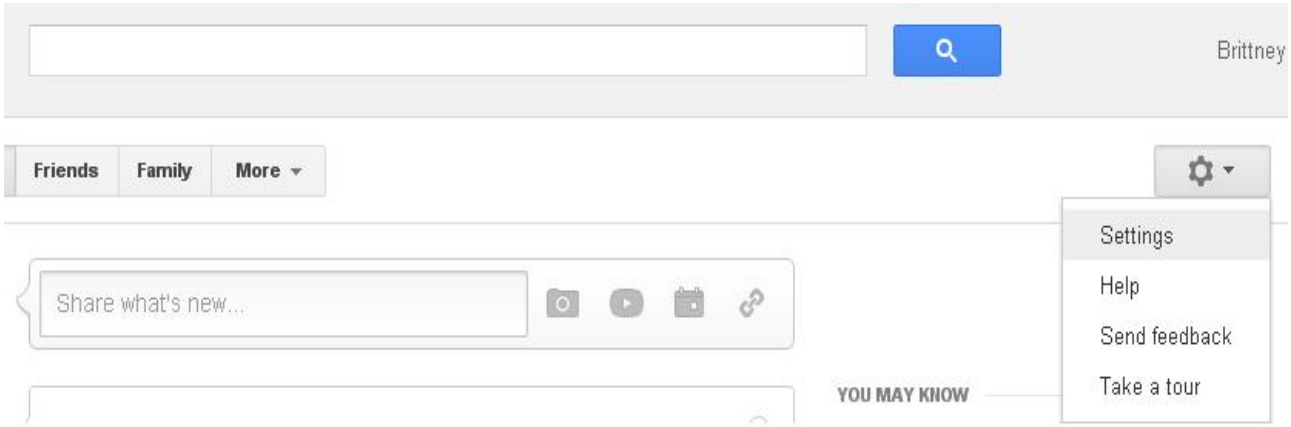

Figure 6: Google Plus Settings Button (Google)

The list of privacy settings that appears once the settings button is selected is quite long. The clear verbiage on these privacy settings is one of the most significant benefits Google Plus has over Facebook. Each setting is described thoroughly so that the user never has to question what the setting does or how it helps improve the privacy of the user's content. For example,

rather than Google just stating that the user can change the visibility of posts, they go one step further remind the user to “Remember that anyone a post is shared with can see all comments to that post, who else it’s shared with, and share the post with others” (Google). Google makes it clear in that statement that posting information presents certain risks and that the user should remember that visibility settings can only protect privacy to a certain extent. Therefore, the user must still be mindful of the information posted on Google Plus. Figure 7 shows just sample of some of the privacy settings available on Google Plus and the associated descriptions for those settings. Unlike Facebook’s vague descriptions for settings, Google Plus makes protecting privacy easier by giving the user sufficient descriptions of all privacy settings.

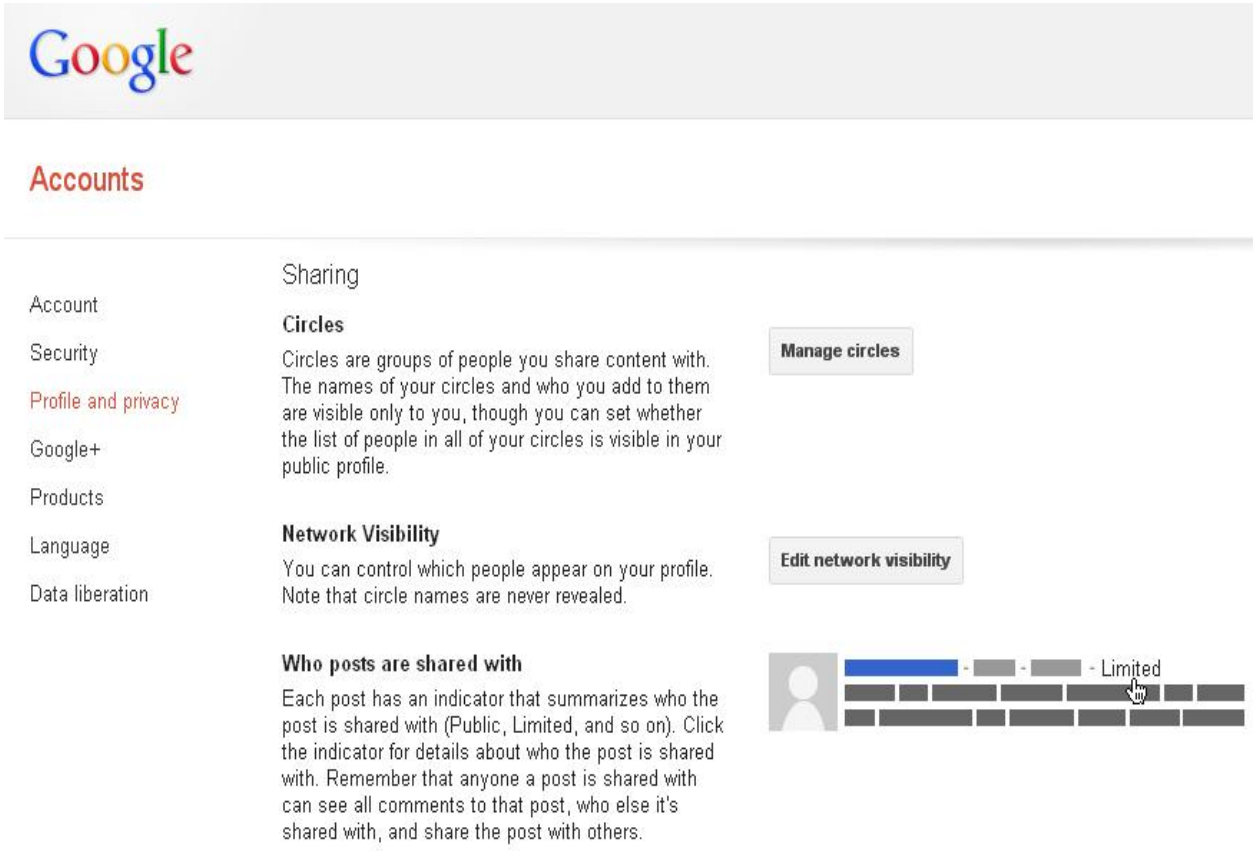

Figure 7: Google Plus Setting Descriptions (Google)

In addition to providing users with detailed description of privacy settings, Google Plus also automatically saves the changes users make to these settings; therefore, users do not have to worry whether or not they selected a "save all changes" button like they do on Facebook. In terms of applications, Google Plus provides users with an option in the security section of these settings to edit what applications can have access and sync to the user's profile. The OSN even includes a link in this area for users who want to know what exactly they are sharing. By giving

users links to privacy policies and information, Google shows that they do value the user's privacy and the ability to protect it.

Overall, the navigational structure and detail that Google Plus provides this page allows users to better protect user privacy without neglecting areas that could be overlooked on other OSN's such as Facebook. Although Google has one privacy policy for all services, the number and quality of the privacy settings it offers Google Plus users makes up for the inability for users to opt out of some Google services individually. As discussed in Chapter Two, users should continue to recognize that Google has one unified privacy policy, so using one service means users are agreeing to the policies of all other Google services.

Twitter Settings

Twitter offers the least amount of privacy settings that users can control. Similar to Facebook and Google Plus, the settings button is found on the right-hand corner of the page. The settings button is the face icon with an arrow facing downward. By selecting this button, users can choose settings and have access to a few tools that are useful for protecting their privacy. As discussed in Chapter Two, Twitter automatically defaults its settings to public. Therefore, any user who wants to make his Tweets private needs to manually change the privacy settings. Users can limit if their posts are publicly available, if they show their location, and can require a password before allowing changes to be made to their account. Figure 8 shows most of the privacy settings Twitter offers its users.

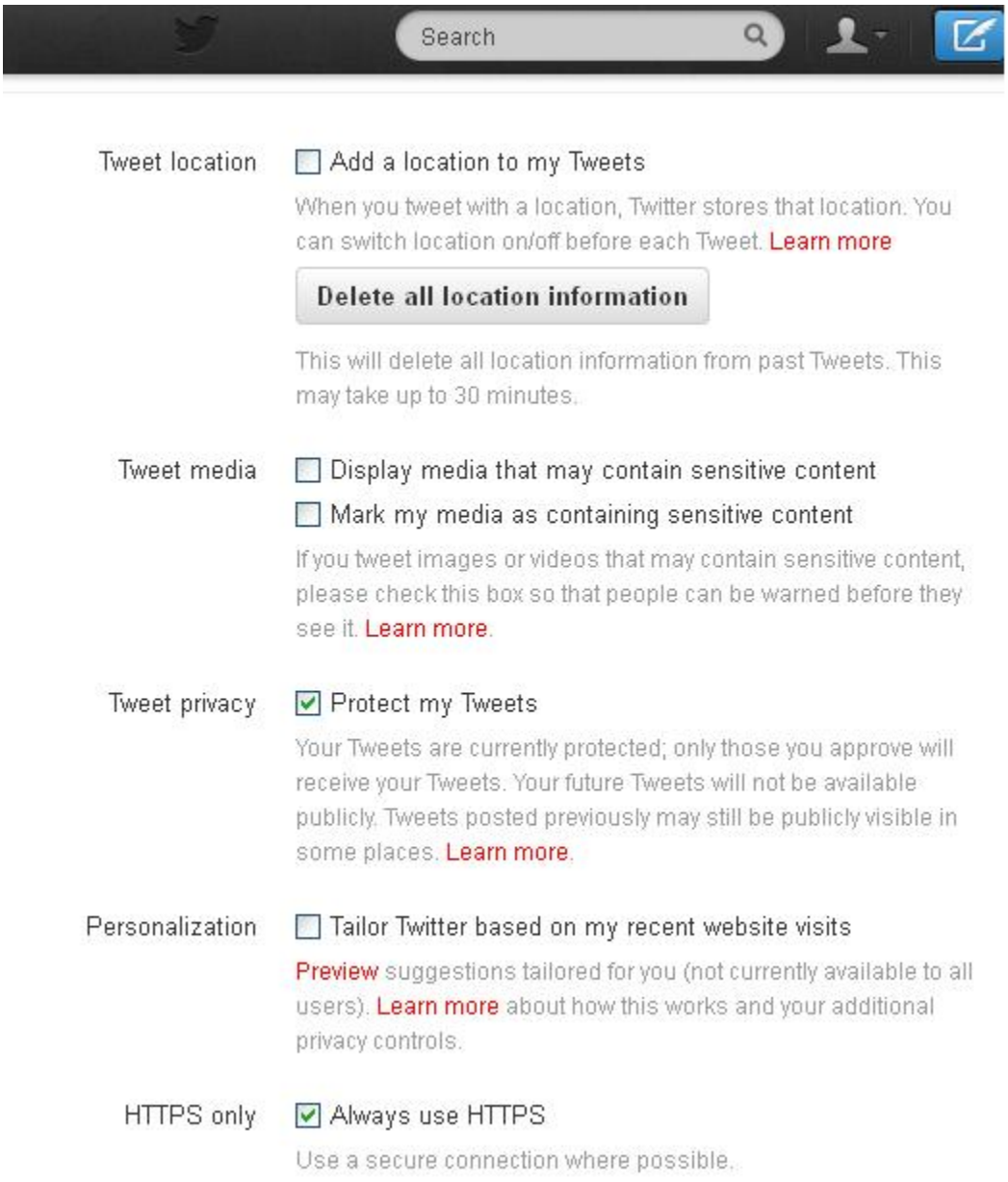

Figure 8: Twitter Privacy Settings (Twitter)

Twitter does provide users with small descriptions that detail what each setting involves. Twitter also has links next to most of the settings so that users who are unfamiliar with the settings or users who just want additional information can learn more. Many of these links lead directly to Twitter's privacy policy, which is convenient for users who want to do some research before adopting any privacy settings to the user's Twitter account. The problem with the privacy settings on Twitter is the fact that very few are available. Users do not have much control over the privacy of personal content. Because few privacy settings exist on Twitter, users should consider protecting the content they can. The most secure way users can protect content and privacy is to select the "Protect my Tweets" option as shown in Figure 8. This option causes all Tweets to be private, except to those audiences that the user wants to share with. For example, a user can post a Tweet and it can only be seen by the person the Tweet was sent to. This is optimal protection for users who post sensitive information that they may not want showing up on their profile, such as R-rated movie clips or posts. Users should keep in mind that even though this option is offered, any Tweets that were posted before the privacy settings were adopted are still public. Thus, users should not assume that all Tweets on the user's account are secure and private.

Users can also optimize the privacy of content on Twitter by selecting the "Always use HTTPS" option on Twitter's privacy settings page. This option allows the user's browser to access Twitter through a secure connection when available. While a secure connection may not always be available, depending on the computer the user is accessing Twitter on, it can cut down on the risk of the user's content being accessed maliciously. Users who access Twitter

through a secure setting should feel some sense security that hackers are not attempting to capture the user's content. Hackers can often retrieve user content when content is accessed through an unsecure connection. Therefore, this is an important aspect of all OSNs, not just Twitter. Users should select the HTTPS option if it appears as an option on the OSN privacy settings.

While the privacy settings are scarce on Twitter, the apps section is much more user-friendly than other OSN's. The applications that the user has connected to his Twitter account are listed under the "Apps" tab of the settings page and have a revoke button that users can select to stop any syncing or access that application has to their account. In contrast, Facebook has a pop-up that users have to select to confirm that they want to delete the application. Therefore, Twitter makes deleting apps from user accounts a simpler process.

Overall, Twitter offers positive contributions to privacy protection with its easy to use application settings, but still presents privacy risks due to its lack of privacy settings. Twitter's lack of privacy settings is concerning because users do not have many opportunities to protect privacy and to control what information is provided to the public. All Twitter users who want to increase their privacy protection should consider what information they want others to see. Privacy settings are available on OSNs such as Twitter so that users can better protect privacy. These privacy settings should not be considered a solution to protecting privacy; rather they should be considered a tool that optimizes what users can do individually to help protect their information and content.

Suggestions for Government Action

OSNs should be held responsible for disclosing and using user information in ways that the user has not approved. There have been many lawsuits against Facebook, most recently one that originated in the state of California. In the lawsuit, "…five Facebook members, alleged the social networking site violated California law by publicizing users' "likes" of certain advertisers on its "Sponsored Stories" feature without paying them or giving them a way to opt out" (Levine and McBride). An example of this situation would be if a user liked a product such as Coca-Cola on Facebook. When that user's friend logged-in to Facebook, Coca-Cola would appear as an advertisement on the page. Below the advertisement would be a description stating that his friend "liked" the Facebook page. The Facebook members that filed the lawsuit in California complained that they were never notified that "liking" a page would appear below advertisements and were displeased that they were not paid or given the option to decline the use of the user's names.

After this settlement, Facebook improved their site to allow users to opt out of this feature, but they did not face many consequences. The lawsuit ended with Facebook agreeing "to pay $10 million to charity to settle a lawsuit that accused the site of violating users' right to control the use of their names, photographs and likenesses" (Levine and McBride). The importance of user rights is continually being overlooked by government and state officials. Facebook needs to be held accountable for their frequent actions that have caused user privacy to crumble. If no action is taken, the precedent will continue and other OSN's may follow in Facebook's footsteps knowing that no serious actions are likely to be taken against them. As

discussed in Chapter Two, the government has let Facebook get away with numerous privacy leaks and the only way to stop it from happening again is to increase the consequences. Facebook should not be allowed to just pay money to make up for putting user privacy in jeopardy. Compliance needs to be enforced because it is clear that monetary consequences are not enough to stop Facebook from putting users at risk.

CONCLUSION

Social media networks need to be held responsible for the privacy issues associated with their use. One of the most significant issues is the content of the OSNs privacy policies. Facebook, Google Plus, and Twitter all have different policies, but they generally address similar topics such as advertising and data collection. Users should not assume that all privacy policies are identical because they do vary considerably. While Facebook has a lengthy policy, it has many sections that do not describe the policies in detail, such as when advertising policies are discussed. Google Plus does an adequate job of explaining policies, but does not offer users the ability to decline the policies of specific services, such as Gmail and YouTube. Therefore, Google Plus users must accept the privacy policy for all of Google's services regardless of whether or not the user accesses those services. Twitter has a satisfactory privacy policy, but does not provide users with many options for protection. Twitter's privacy policy is standard and does not go the extra mile to provide users with specifics or options that could help improve user privacy, such as including explanations for why user content cannot be made completely private.

Overall, Facebook, Google Plus, and Twitter could learn a lot about what their privacy policies are missing in terms of details and options if they simply completed a comparison of the network's privacy policies. Users benefit the most from comparing the privacy policies because they can determine which OSN has the most prospects concerning the protection of user privacy. Users should keep in mind that no OSN can entirely protect user privacy because

of the plethora of features OSNs make available each year. Users take a risk using OSNs and their features, specifically, risking the invasion of privacy. OSN users are ultimately responsible for what content is posted on OSNs and what features are used. This responsibility is not only a crucial point for OSNs, but also for the social media applications that often link to these OSNs.

Social media applications do not provide users with enough information regarding how content and information are retrieved or dispersed. Because adequate details are not provided to users, it is the user's responsibility to research applications before allowing them to access content. Permissions are requested before the user downloads an application. Rather than being a creature of habit, and assuming that the permissions are harmless, users need to read the permission's description carefully and refrain from accepting any permissions that seem questionable. Permissions should particularly be avoided if they feature requests that attempt to access the user's microphone, record audio, make phone calls, or access the user's location. While some of these permissions could be used without malicious intent, the user should approach requests with caution so he can decrease the chance of privacy invasion.

Users should also be aware of the social media applications activated directly through the user's OSN. Applications that are accessed through Facebook and Google Plus may request permissions similar to the phone version of the application. The permissions requested on OSNs could require the user to allow the application to post on his behalf, have access to the user's email address, or access the user's personal contact information. Because social media applications are not always created by reputable developers, users should understand that

anyone could be the developer behind an application. Independent application developers are common and often appear anonymous. Users should make an effort to not only read the permissions requested before download, but also pay attention to the developer's reputation. If the application is unfamiliar or seems too good to be true, it probably is. It is up to the user to be responsible and use discretion before downloading social media applications to his phone or OSN profile.

Because OSNs and social media applications have many aspects that affect user privacy, the importance of the user conducting research cannot be stressed enough. The only way for a user to understand why OSNs put user privacy in jeopardy is to read the privacy policies frequently for changes and to research the OSNs themselves. A simple search in any online search engine retrieves a sufficient number of results that can give the user more insight as to what is being said about the OSN in regards to privacy. OSNs are frequently in the news regarding complaints and controversies associated with their use. It is important that users understand that no OSN is perfect. Each OSN has different features, policies, and options, and it is up to the user to discover what they are and how they fit into the user's expectation of privacy.

Facebook, Google Plus, and Twitter are just some of the OSNs that exist in 2012, and users of all social media networks should become more aware of the privacy issues associated with each OSN. Although all three of these OSNs have power in the number of members they have, power does not mean that the OSN presents no risk to the user and his privacy. Being

aware of privacy issues such as account information leaks, the selling of user content to third-parties, and what becomes of deleted content, are just some of the privacy risks users face every time they log-in to an OSN. By analyzing the views of researchers and the studying the privacy policies of OSNs, users can make a more educated decision about what privacy means to the user and if the OSN offers protection against the issues that matter most to users. While there is no method to being completely protected from privacy issues, there are a number of methods that can be used to protect user privacy.

Users can apply privacy settings to OSN profiles that limit what other users can access or view on the OSN profiles. These settings vary depending on the OSN and are often not easily viewable by the user. However, users can research the OSN or make a profile, and simply investigate how privacy settings can be changed and what features the OSN offers to users for privacy protection. Users should read the settings carefully and should not approve any settings that expose user information to the public in ways that are startling. If the user finds a setting that makes all of his content publicly available or that shares information with advertisers, that user should consider the consequences of having content exposed. While users have an expectation of privacy, some users value privacy more than others. Users who do not mind having personal information used or sold should keep in mind that anyone can view their content. For example, a user that has a public profile can be searched by people such as prospective employers, friends, and strangers. The nature of this privacy issue is dependent on what the user values and his concern with what anyone can find out about him. All users should think twice about what content they allow OSNs to access and be cautious of posting

information that the user does not want certain people to see. OSNs have settings to help protect privacy, but there is no way for them to ensure that the information and content will never be compromised in the future.

Social media has a profound effect on privacy because it is directly changing the way users act on the Internet. Some users are concerned about who can access personal content, while others are concerned with not being able to express themselves freely. Social media is undoubtedly a field that is not going fade in the near future. Therefore, users of all ages and experiences need to become more aware of what OSNs have access to and what it done with user content. By becoming more aware of privacy issues, users can urge changes to be made to the way social media is approached in the United States and around the world.

WORKS CITED

"About Facebook Advertising." Facebook. , n.d. Web. 25 June 2012.

Acohido, Byron. "Social-media Apps Raise Privacy Concerns." USA Today n.d., Academic Search Premier. Web. 12 June 2012.

Acohido, Byron. "Facebook's New Features Remain Unpopular." *USA TODAY* 17 October 2011. Web. 30 Jan. 2012

"Android Developer's Guide." *Android*. Google. , n.d. Web. 17 June 2012.

"Android Reference." *Android*. Google. , n.d. Web. 17 June 2012.

Angwin, Julia, and Jeremy Singer-Vine. "Selling You on Facebook." Wall Street Journal. WSJ, 10 Apr. 2012. Web. 21 June 2012.

Boyd, Danah M., and Nicole B. Ellison. "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13.1 (2008): 210-30. Web

Chen, Guanling, and Faruq Rahman. "Analyzing Privacy Designs of Mobile Social Networking Applications." *Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference*: 83-88. *IEEE Xplore*. Web. 21 June 2012.

Debatin, Bernhard, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences." *Journal of Computer-Mediated Communication* 15.1 (2009): 83-108. Print.

"Discover Android." *Android*. Google. , n.d. Web. 17 June 2012.

Dwyer, Catherine, Starr Hiltz, and Katia Passerini. "Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and Myspace." *Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado, 9-12 August 2007*. Web.

Enck, William, Machigar Ongtang, and Patrick McDaniel. "Understanding Android Security." *IEEE Security & Privacy Magazine* 7.1 (2009): 50-57. *IEEE Xplore*. Web. 20 June 2012.

"Facebook Ads." Facebook. , n.d. Web. 25 June 2012.

"Facebook Data Use Policy." Facebook. , 8 June 2012. Web. 29 June 2012.

"Facebook Help Center." Facebook., 8 June 2012. Web. 29 June 2012.

Federal Trade Commission. "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises." Federal Trade Commission. November 29, 2011.

Fredreka, Schouten. "High-tech, Social Media Companies 'Friend' Politics." USA Today, n.d. *Academic Search Premier*. Web. 12 June 2012.

Friewald, Susan. “First Principles of Communications Privacy.” *Stanford Technology Law Review*. 3 (2007). Web. 28 June 2012

Hugl, Ulrike. “Reviewing Person’s Value of Privacy Online Social Networking.” Internet Research 21.4 (2011): 384-406. EBSCO. Web. 31 Jan. 2012.

Lenhart, Amanda, et.al. “Teens Kindness and Cruelty on Social Network Sites.” Pew Internet & American Life Project. 9 Nov. 2011. Web. 19 March 2012.

Levine, Dan, and Sarah McBride. “Facebook to pay $10 million in user lawsuit.” Reuters. MSNBC. 17 June 2012. Web. 27 June 2012.

“Manage Your Account Privacy.” Facebook Help Center. Web. 05 June 2012.

McAuliff, Michael. “Facebook Protection Amendment Voted Down in House.” *The Huffington Post*. The Huffington Post.com. 27 March 2012. Web. 12 June 2012.

O’Brien, Kevin J. “Austrian Law Student Faces Down Facebook.” *The New York Times*. The New York Times Company. 5 Feb. 2012. Web. 19 March 2012.

Page, Larry. “2012 Update from the CEO.” *Google Investor Relations*. Google, n.d. Web. 17 June 2012.

Paul, Ian, and Brent Rose. "Smartphone Spying Reality Check." PC World 29.7 (2011): 13-15. Academic Search Premier. Web. 21 June 2012.

“Google Policies and Principles.” Google. , n.d. Web. 05 June 2012.

“Privacy Settings.” Facebook., n.d. Web 25 June 2012.

“Twitter Privacy Policy.” Twitter. 17 May 2012. Web. 05 June 2012.

Tsukayama, Hayley. "Google Privacy Policy Is Subject of Backlash." *The Washington Post*. The Washington Post, 25 Jan. 2012. Web. 5 June 2012.

Smith, Aaron, and Joanna Brenner. "Twitter Use 2012." *Pew Research Center's Internet & American Life Project*. Pew Research Center, 31 May 2012. Web. 05 June 2012.

Yadav, Sid. “Privacy on Social Networks A Concern For Old, Not Young.” *VentureBeat*. Venture Beat, 11 Nov. 2010. Web. 05 June 2012.