2013

Facebook policy and user knowledge: Self-inflicted totalitarianism

Richard Rockelmann Jr

“Facebook Policy and User Knowledge: Self-Inflicted Totalitarianism”

By

Richard W. Rockelmann Jr.

Project submitted in partial fulfillment of the requirements for the degree of Master of Science in Networking and Systems Administration

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

Department of Information Sciences and Technologies

2013

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

Master of Science in Networking and System Administration

Thesis Approval Form

Student Name: Richard Rockelmann

Thesis Title: "Facebook Policy and User Knowledge: Self-Inflicted Totalitarianism"

Thesis Committee

Harris Weisman

Richard Mislan, PhD

Jonathan Maurer

Acknowledgement

There are many people that I would like to thank for supporting me on my long journey up to this point in my life. First and foremost I would like to acknowledge my family, as my Mother and Father and Grandparents have been there through the thick and thin of both my educational and personal journeys. I would be nowhere without the support and the ideals they have instilled in me since I can remember.

Once moving on from high school and the more direct support from home, the Rochester Institute of Technology supported my educational journey in ways that I never expected. I would like to thank all of my teachers along the way for their patience and understanding. Without them, I never would have achieved this much in my academic career. Furthermore, my Masters Thesis would not have been able to be completed without the support and encouragement of Harris Weisman, Richard Mislan and Jonathan Maurer. I selected them to be my Thesis Committee for many reasons but overall because I look up to them and their support was, and is, greatly appreciated.

Finally, without the emotional support from my friends there is no way I would have actually finished this research. I would like to thank Kyleigh Van Dine and Joseph Sciandra Jr. for their constant support and encouragement with my personal and academic struggles. I wish them the best in their future endeavors.

-Richard W. Rockelmann Jr.

Abstract

Facebook has become an integral part of digital natives lives. As the technology is used more often, trust in the service increases. The unfortunate reality: people misinterpret trust by assuming anything can be said and done on this popular social media outlet. The problem of course is the fact that Facebook is a business that is fueled by sharing information to both third parties and other people. Their business scheme, combined with users misunderstanding of what power the policies have over them has the potential to incriminate and destroy students future they are working so hard to obtain. Are people actually okay with sharing their personal information online or is there a disconnect of what they understand? This study focuses on the policy knowledge that college students at the Rochester Institute of Technology have and tries to gain an understanding if education is able to sway users to relinquish a bit of social ability to conserve their privacy. A survey was given to 110 subjects which asked qualifying questions then educated them of the security concerns and finally asked a set of questions to gain a before and after picture of what they have learned. This before and after comparison proved that users in this day and age prefer being socially connected rather than taking needed steps to lessen online risk and overall have fallen subject to the disinhibition effect.

Table of Contents

List of Tables

List of Figures

Overview

1.1.1 Research Motivation

In recent years humans have entered an entirely new world with new ways of interacting with each other. Throwing away conventional means of communication, we now surround ourselves with online communication and social connectivity. On the surface, these new communication methods, such as Facebook, seem like a great way to stay in touch with others, interact with long lost college friends or even brag about a new car to show the world that hard work and dedication paid off. The problem however, is in the manner in which this new communication is handled. Face to face interaction is something humans are accustomed to and understand as we naturally acquire these skills as we grow and experience life. Reminiscing about my time in college and how much I have learned about online activity in regards to the security and privacy of such, I started to wonder how many people actually understand the implications behind what they do online. Meaning, what kind of cognitive processes do people have when they act on Facebook and why is there a lack of censorship when people post and intermingle on this common social networking website.

During my freshman year, Facebook was the place that I would write (post) any of my naive thoughts without thinking twice. Many people like myself, I feel really had and currently have no concept of any possible repercussions that might result regarding what they post. Typical statuses can be about personal information, and others can be about a horrible waiter at a local Applebee's. However, what many fail to realize is many posts and interactions can really can

do some damage if the right people gain access to the updates that are so often posted without thought due to the disinhibition effect. Ironically, being online creates a virtual security blanket around users and makes them feel as if nothing can touch them no matter what they post or do. However, the skeptical, and those who are a bit more frugal with their actions, understand that their presence online is just as, if not more implicating than acting similarly in person. Every application that we use has a user agreement and a privacy policy that has to be agreed upon before that application can be used. How many people understand what these are and how they can be used to implicate them? Proceeding through day to day activities how can one be sane knowing that at any moment the world has access to the most intimate details about your life; It is simple as going online and legally accessing your information.

For some people, pursuing the Facebook pages of strangers is pure fun and for social enjoyment, however, for others, it is the first step of many methods in which begins a series of potentially implicating actions. Only seventy percent of people signing up for any service actually read the user end license or policy agreement. And of those, an average of six seconds is spent on the page that tells them, as in Facebook's case, who has access to their information, what can be done with it, and who has the intellectual rights to the media that is posted on Facebook servers. (Böhme, Köpsell)

Once I read and understood this information, and realized the actual resulting use of my personal information, I was astounded. The later caught my attention and fueled my desire to understand fully what readers can actually

grasp about other users online activity relating to their security. We are living in the generation of virtualized communication, however, people take what they know instinctively as an intimate conversation and post it online thinking the same intimate details shared in person are safe for all to see online. My goal is to understand what needs to be expressed to College Facebook users in order for them to have a better understanding of their actions on Facebook. Hopefully, this information will be effective and help to change the way they communicate and post about themselves, thus creating a more stable, secure environment.

Background Information

2.1.1 “1984”

Totalitarianism is a term coined by Benito Mussolini, and later the famous author George Orwell in his book “1984” used the term, placing a new spin on the definition. “1984” is a story about the government controlling every aspect of a population’s lives with little or no control placed in the hands of the people under its society. The Government managed to place each and every inhabitant under close surveillance; if they did anything against the ideals of the nation, serious consequences would unfold for them.

Totalitarianism as defined by the *Business Dictionary* is a political structure that involves the population of a country being entirely subject to the government’s absolute authority in pursuing its goals. Carrying on normal business and personal activities under a totalitarian regime can be challenging since government agents and the police often act without being constrained by normal legal procedures. Today in our day to day lives, the concept of totalitarianism remains consistent, however, the government, without the use of completely illegal methods, are able to use what is available to them to monitor its citizens by using completely legal methods called Facebook and Social Media.

"There was of course no way of knowing whether you were being watched at any given moment... It was even conceivable that they watched everybody all the time. But at any rate they could plug into your wire whenever they wanted to. You had to live – did live, from habit that became instinct - in the assumption that every sound you made was overheard, and except in darkness, every movement

scrutinized.” (George Orwell, *1984*) This quote can relate to our society today as people are giving up all of their private information to Facebook and other online mediums by their own free will. Self Inflicting Totalitarianism is the exposure of personal information, willingly through any online outlet, supported by policies that are in place and that many do not understand.

The problem is not that people are using these applications, but the fact they do not know how the technology is used in order to better understand them as a whole. Giving up information online enables people and organizations to gather or derive personal data about an individual without their knowledge. Totalitarianism, while it is not blatantly part of our lives, is intertwined into what we call the Internet and is fueled by the very people that would never want to give up the information they willingly provide to the world through social websites to their enemies or people they do not know.

2.1.2 Technology Evolution: Machine and Man

Ever since Simon was the name given to the first "personal computer” in 1950 (Callis) computing technology made rapid advances. From Simon to the Apple II and beyond, computers are rapidly changing and so are the people that use them. Is it reasonable to say that the very machines we use are changing people? Back in the early 80’s not so much, however, with the steady increase of the numbers of computers purchased from a mere 48 thousand in 1977, to 125 million in 2001, it is safe to say something is fueling this popularity. (Kanellos)

Finally, the release and final grounding of the Internet caused the popularity of personal computers and other supporting technology to

exponentially grow. The release of the Internet was something that enabled people not only to complete work faster, it also fascinated them with the almost instant communication they could have with people thousands of miles away. It is safe to say that this technology took the definition of a personal and intimate conversation and transformed it into a digital superficial dialogue. Back in the 80's and early 90's people were first starting to adopt personal computers and the Internet. Furthermore, the technology was overall looked at as a resource and something that was used and then left to sit while other tasks were finished and other day to day activities were completed. Those who adopted the computer during that time were not sure of the technology and were not completely comfortable with it. Much like an Immigrant moving to a new country and feeling intimidated about the foreign language and people, early adopters of the computer did not understand and understandably were a bit fearful. "These Digital Immigrants learn - like all immigrants, some better than others - to adapt to their environment, they always retain, to some degree, their "accent," that is, their foot in the past."(Prensky) Comfort comes from a long process of using and understanding any new technology. At that time people never trusted them, which explains the sporadic usage only when completely necessary reverting back to what they understood by leaving the newly adopted technology alone when they did not have an absolute use for it.

More recently the "digital immigrant accent" can be seen things such as turning to the Internet for information second rather than first, reading the manual for a program rather than assuming that the program itself will teach us to use it.

Today's older folk were "socialized" differently than their children, and are now in the process of learning a new language; a language learned later in life, scientists tell us, goes into a different part of the brain. (Prensky) Part of the unknown creates a trust issue while using it. Furthermore, the “accent” can been seen in many other more common examples; a desire to print out an email and save it or the need to print out a document because you need to make changes or edits before a final revision is done on the computer.

Overall the mindset of people who did not grow up on the computer and the Internet is firm, using it as a tool and a way to get things done which can mean sending a quick communication or sending an email. Typing out the work report due soon or sending an email are typical accomplishments done by Digital Immigrants. These are the people that look at the “kids” of the day and wonder how they spend 24/7 sitting in front of a computer or on their phone. These “kids” are not different from those of yesterday, but this generation, takes on a new name called “Digital Natives.”

Digital Natives are those who grew up with and continue to use technology such as the internet, Facebook, Twitter and Google; they do not know what a book is other than a tool they use reaching the end of their search on Google. As a Digital Native the mindset changes when it comes to using a computer and the Internet. Such are no longer used as a tool but something that is integrated into their lives as a necessity. The lifestyle and now a culture have become ingrained in them both socially and emotionally. “Today’s students - K through college - represent the first generation to grow up with this new technology. They have

spent their entire lives surrounded by and using computers, video games, digital music players, video cams, cell phones, and all the other toys and tools of the digital age. Today's average college grads have spent less than 5,000 hours of their lives reading, but over 10,000 hours playing video games (not to mention 20,000 hours watching TV.) Computer games, email, the Internet, cell phones and instant messaging are integral parts of their lives." (Prensky)

The fact that children have grown up using the very technology that now controls their lives reflects the overall mindset concerning the internet and technology and their uses; it changes in comparison to their parents before them. How an individual learns aside, the manner in which people view anything and behave overall is very much dependent upon what is around them. This causes the output of their thoughts and their actions to change dramatically. When it comes to the internet and personal computers, the main modification of thought is the ability to trust what is done on the internet which translates to the level at which people care about what they do and say on Facebook.

2.1.3 Self Infliction Cause

According to the Pew Internet and American Life Project, current College Students are early adopters and heavy users of the Internet and compared to the general population they are more likely to be online. (Smith, Rainie, and Zickuhr) Current College Students are those who purely grew up on the technology around them by being surrounded all of their life, immersed since birth. It has even become comparable to an additional limb and something required to perform any activity. They use the Internet for things such as checking email

while having multiple addresses, browsing for leisure, downloading movies, music and photos. It also is used for education for contacting professors, research, collaborating with fellow students and working on projects. (McMillan, Sally J., Morrison) Students also reported in and explained recently, a use for social communication, entertainment and to easily and practically to stay in touch with friends and family. (Smith, Rainie, and Zickuhr) Of course many other uses are out there such, to find relationships, maintain gossip, and to purchase their favorite brand name computer, however, the sky is the limit regarding today's version of the internet and its supporting technology.

The gravity of how deeply technology has intertwined the minds of young people is somewhat unexplainable, resulting in a new kind of social knowledge and skill that those before them had no way to fathom. The old school and new school social views have been an argument among parents and kids for as long as humans have been in existence. However, this generation "may well be more literate, creative, and socially skilled because of their early familiarity with the internet, including trying out various aspects of their developing identity online." (Rice)

Take a moment to think about how friends are made, and the process that is essential to making friends and bonding. Spending meaningful time with them is crucial to start to learn about one another and develop a bond. Over time an attachment occurs and eventually new friends find themselves telling each other everything about each of their lives. Understanding that there is mutual trust, the expectation is that the information you share with each other will be never be

compromised. A natural trust and bond that most cannot explain, grows between persons who are a close part of each other's lives. However, sometimes a relationship is not built on trust and like those relationships the technology that college students and children use cannot be trusted to the extent that those using it have become accustomed.

2.1.4 Facebook: The Addiction, The Cause

Consider a friend in whom everything about one's life has been shared. This friend in whom confidences were shared because of the comfort level shared between you. Think about what could happen if each and every piece of gossip or private information you revealed, or had a discussion about, was made public for all of your mutual friends and their friends to see. As previously stated, this generation may be more socially skilled because of what the Internet has to offer and what kind of activity people can do while surfing the web. The problem ensues when that hyperactive social skill, which genuinely was created by a network of websites and social engagement, becomes mixed with a website that feeds, and prospers off of the ability and user willingness to share basically every aspect of their lives.

Piotr Sztompka explains in detail the possibilities as to why people have developed the level of trust they do while being online. He also outlines that the level of trust has a limit when interacting directly with people rather than freely and openly broadcasting. In part, online activity has become less restricted and private due to the fact that "large aspects of contemporary life have become opaque; increasingly, individuals were dependent on persons whom they did not

know; and the ‘growing range of options in all domains of life meant more choices and more uncertainty.’”

The counter argument of course would be as follows. Could it be that people are just the same socially as they have always been, however, the internet and tools such as Facebook and other social websites have simply given another outlet to “be themselves” and express what they are feeling? As stated, when speaking one on one with someone unknown through the internet, there is still a level of distrust and concern. But when expressing though a medium that is broadcast there is no concern at all. Today on Facebook, there are a variety of comments made (posts) but nothing more or less than anyone ever expressed to their friends or people they know as “acquaintances.”

For example, just a few short years before the social networking hype when someone were to earn their driver’s license they would show it to all their friends and acquaintances at school, and at their workplace. Naturally, others would overhear and they would recognize the person they know has a license, and move on. Today, the same process occurs, but also includes Facebook. Facebook today is inherently the sum of all one’s friends and acquaintances. The audience number increases then exponentially, and to make matters worst on a more permanent place. Thus, not only do they show off their license in person but they post a picture of it online creating a place for the confidential numbers and information to be stored permanently for all to see.

Normally, there is nothing overly concerning when revealing personal information such as a driver’s license in person. However, people transfer the

same feeling of normalcy and apply it online, that is when security and problems occur related to personal information that is now shared, stored and known on the internet. Research has shown that personal variables are transferable from "in person interaction" to "online interaction" and how they share information. Extroverts of course, are more gregarious, friendly and more active socially; they also have been found to have more elaborate social networks and pages. (Engelberg, Sjöberg)This would most definitely translate to how much and what they share online as well. More extroverted people have no problem posting anything regarding their actions such as pictures of a party or their most recent accomplishments. On the contrary, people who are more introverted "in person" have a smaller social circle online, however, this does not change the kinds of information they share.

The differences between the introvert and extrovert personalities are the reasons behind sharing the method they each choose. An Introvert shares because they may want attention, or they hope to gain friends through an easier method than actual personal contact. The extrovert shares because they want everyone to know about them. At the social core, the differences are insignificant and come down to basic human nature; we all want to be part of something and all want to feel liked. Facebook allows for both types of people to satisfy easily that simple desire

2.1.5 The Disinhibition Effect

Aside from what kind of person you are, being online makes all users susceptible to something called the Disinhibition Effect. Virtually all of the Digital Natives and most of the Digital Immigrants have been guilty of doing something in accordance with this theory mostly because we feel a “security blanket” is around us while communicating online. The Disinhibition Effect is the loss of social restriction and inhibitions that would otherwise be present in a normal face-to-face interaction or during a conversation or any form of online activity. (Suler) According to research, this is due to many factors but have been summarized into a few well defined reasons as to why we act the way we do, and why face-to-face interactions differ from those we have online. According to John Suler, people self-disclose or act out more frequently or intensely online than they would in person. (Suler) Understanding that each individual online user is different the following summaries explain possible reasons why people in general are more open online than in “reality.”

While online, especially when connected with Facebook, people feel that they cannot be identified the same way they can as in public. This anonymous feeling gives us a sense of disconnection from the real world and lets us behave in new and exciting ways that in “real life” we would never think of. (At least with people that do not know any better). (PSY Blog) “Because of the online Disinhibition Effect some share too much on their social networking profiles, sometimes even things they wouldn't admit to their closest friends. It's easy to

forget that you don't need espionage training to type someone's name into Google. (PSY Blog)

Furthermore, people develop a sense of invisibility that enables them to express themselves more freely through the keyboard. Instead of worrying about facial expressions and body language while talking face-to-face, or being concerned about the emotional signals the other person is portraying, we feel it is easier to disclose information through a keyboard, effectively removing ourselves from the other persons unknown reactions. Online, we can express the whole conversation without stopping because of the urge to hide our emotion from the person we are talking to. People are overall afraid of what others think and witnessing any sort of negative cue or feedback immediately causes us to shut down. Humans like to share information, and for those afraid of what people may think, Facebook communication has become a great outlet.

Posting a frustrated status about an individual is very common today on Facebook. Frequently, people use statuses to indirectly converse or cry for help regarding a personal matter. The asynchronous effect of being online is appealing because it allows for portraying the message without having to deal with the immediate reaction of the person you are speaking to or, in the example, trying to get the attention of. (Suler)

Currently, seventy percent of Americans play video games. This is an astounding jump since 2007 when a mere forty two percent were active in the video game scene. (Rideout, Victoria J., Vandewater, and Wartella) For many people, being online is just like another video game. Online activity can be

associated to the feeling of a video game because so many play them and because the use of any technology gives the impression of a fake world. However, this does not change the dangerous fact that people feel their online communication need not have any censorship. People think that once they are logged off and back to “reality,” they can leave behind it all behind and not think about what happens in that place they feel is a “fictional reality.” This inevitably can create potential legal problems as online users overall do not have a sense of authority. This inevitably causes users to continue to behave in a manner in which is not fitting of their personal brand.

Due to the fact that Authority Figures express their status and power by their dress, body language, and in the trappings of their environmental settings, the absence of these cues in cyberspace reduces the impact of their authority. (Suler) The reality is, while online, a false sense of a level playing field has been created, therefore, resulting in out of the ordinary thoughts and actions due to its seemed anonymity and private nature. With reference to previous points, people are afraid to say what they think in person especially to an authority figure, because the level playing field exists online, authority simply disappears and so does any remorse of what is posted and talked about through the computer screen. Additionally, because the Internet has no centralized control, unlike the communities we live in, the seeming lack of authority amplifies because of the volume of internet users. People believe the possibility that government agencies, acquaintances or other organizations view potentially incriminating

information are so miniscule that their actions will have no negative repercussions.

Each of the explanations for lax internet behavior cause a different set of problems which inherently, on Facebook, are publicly displayed. Anyone who uses this popular social media tool needs to know the possible resulting consequences of such behavior. Understanding, and explaining the associated effect of the incriminating behavior overall is important to understanding the site and how to protect oneself.

2.1.6 Facebook: Company Gain Based on You

As summarized above, users are unknowingly naive when it comes to the use of a computer and the Internet and the feeling of invincibility seems to be the overall state of mind while operating a computer and using the Internet. Partially due to a lack of understanding and knowledge, people know how to perform the tasks they want to do, and can do so quite well. However, it would benefit them to know how certain actions result in information, while they are not actively tracked, that can be accessed at any time from virtually any entity.

Google is used everyday by students and professionals alike. What most do not know is that their actions and searches are actively stored and logged. The danger of course is in the searches themselves, especially if they are potentially incriminating. While tracking is concerning enough, Google does not keep records to expose their users, nor does the company relate to “Big Brother.” However, because Google opts to keep tabs on each of its users in order to provide appropriate ads, relevant searches, and location data based on what

users search, it enables Google to not only make more money on ads, but it is also a means to keep the user around longer. However, what most users do not know is that the data stored about them creates a profile of much personal information including actions performed online that one may not want the world to know. Unknowing to many, Google has an entire profile on each user, much like a police case profile. The profile contains one's location and data, (searches) stored to provide you with the best information possible. (Google Support) At first glance many people would assume this is a huge breech of their privacy and they may feel insecure. While this assumption is not incorrect, it is a completely legal way for Google and other companies to take advantage of user data to expand their business.

No different from Google, Facebook takes part in similar actions based on the profiles of friends, pictures, posts and your location data off of your mobile Facebook app. While Facebook has the front of a "Social Entertainment" website the company is not different from any other, it needs to make money and grow into a healthy and survivable corporation. This happens at the risk and the of its users. Each of the posts that a user makes are scanned and sorted though a computer system that guarantees ads relevant to you. (Perlman) Pictures are free to be used by Facebook for ads and promotions, and technically, once uploaded, they belong to Facebook. Furthermore, the company is free to use anything posted or talked about as their intellectual property; they have the power to do much more based on all the data that is willingly provided to it each

and every day. Facebook is constantly changing its privacy policy to allow its users profiles more open to others.

Facebook and Google are just examples of companies that gain from the end user's personal information. Virtually any company online similarly gathers and distributes information. Most users think that this is a violation of their privacy and illegal use of their personal information. Unfortunately, each and every service a user signs up for online shares data in a manner that is completely within their rights as a company. The fact of the matter is sharing information is the forefront and main source of income for them. Protecting yourself from such actions comes with understanding the User End Agreement and Privacy Policy that each and every person must agree to when starting a service.

2.1.7 Privacy Law Online

The government of course has privacy laws based on the way that we interact and how companies collect our information. These laws protect us from many things, however, because of the way privacy policies are constructed, they leave us exempt from much of the data collecting and vulnerabilities. The unfortunate realization, through research, reveals while the government protects our information, the laws are not formatted or even written to prevent data collection unless, the information is regarding medical records, or finances. "Some laws that do protect the privacy of information do not currently extend to casual information searches on the Internet or to information revealed by the user." (Pipes) The solution, in order to protect yourself, is to read and

understand the Privacy Policy for each of the services you sign up for. Each state has their own version of a law "protecting" your information, however, most states, such as Pennsylvania, Nebraska, Connecticut and Tennessee can be summarized in one sentence. The law "Prohibits Privacy Policy to document false or misleading information." (*NSCL)* This means if it is documented in the privacy policy the fact is the company will use your data to its full advantage.

Laws cannot change the fact people simply do not understand what each of the services they use can do with the information willingly provided to both the company and other users. Facebook, unfortunately does not change this revealing conclusion. They use and provide almost every possible piece of information to everyone that can see based on the privacy policy provided to its users. This creates security implications such as but not limited to, identity theft, future employment complications, legal action and phishing attacks. It is very important for users to understand such repercussions based on the information shared.

In my study, I will educate Internet users on the Campus of Rochester Institute of Technology, by way of using a survey. From their responses, I will study their reaction based on the correlation of the information they provide on Facebook and my supporting Policy findings on what they admit to sharing. Their reaction to the information will be key to understanding what it will take to educate users to the point where they will want to change their behavior based on facts that can, and often do, occur every day based on Facebook user data

Literature Review

3.1.1 Previous Work and Research

Facebook is quite possibly the largest social networking advancement since MySpace and has rightfully gained quite a bit of attention from researchers and security professionals alike. Most research, however, is based mainly on the policies and what they can do to the people using the service. The main disconnect is found when research of policy meets user interaction and behavior. Little or no research has been completed to understand the reactions of real users while facing real world examples of such implicating security policies created for the company, at the risk of the user. Much research however, has covered the policy evolution of Facebook and its competitors as well as the steps needed to make your personal Facebook page the as secure as it can be. Furthermore, regarding overall behavior and interaction a significant amount of information has been found regarding specific online Facebook activity.

According to Marshal McLuhan “the self-definition of a culture/person can be traced to the media that the culture relies on.” This makes sense because as a society we are very impatient and demand to have information delivered to us quickly; we have become accustomed due to the fact we have nearly instant access to a wealth of information. (McLuhan) This self-definition, as McLuhan has researched, is about how people react in a changing media society. Facebook has obviously changed over the years and from completed

studies it seemingly has weaned users into what they accept today as a satisfactory use of their information.

3.1.2 Weaning Users off Privacy

It is hard to believe that the following is an excerpt from the policy that Facebook once provided to its users.

> "No personal information that you submit to TheFacebook will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings." (Opshal)

According to Kurt Opsal, this statement was on "TheFacebook's" privacy policy page in 2005 when the website first became popular to college students. Mark Zuckerburg, the founder of Facebook, has stated that the world is changing and is becoming more public and less private. Researchers have speculated this statement justifying why Zuckerburg has purposely taken users down a path of sharing information for company and personal gain. (Kirkpatrick) Research and analysis of Zuckerburg's statements over the years make Marshall Kirkpatrick think that this was a play to force people into more comfortable mindsets while using the technology.

Kirtpatrick has a research paper regarding the issue and he concludes, based on information he has discovered, that Facebook is making a big mistake by veering from its original privacy policy and its concern for users. There are many reasons why Facebook's ever changing policies are a problem for users and Kirtpatrick explains in detail, outlying three main reasons Facebook is doing users an injustice, and why people should discontinue use of the service.

“Evolving Preferences Don’t Justify Elimination of Choice.” Zuckerburg is most definitely correct in that users are changing and evolving. However, this should not take away the right of the user to choose what is private and what is public on their page. Kirtpatrick goes on to explain that privacy is a basic human right and while it may seem less true when we are operating on websites like “Facebook, the users cooperation was once based off of privacy and changing it after users were told it is secure leads them to believe that Facebook always will be secure.” (Kirkpatrick) While Zuckerburg seems to think that privacy is not something desired in this day and age there are groups of people who would benefit greatly to a more secure Facebook, not only emotionally but physically as well. Privacy keeps those who escaped abusive relationships, people who fear losing their jobs, victims of bullies and many more groups of victimized people safe. (Kirkpatrick)

Since 2005 Facebook policy has evolved from “we will keep your data to those who you want to have access to it,” to the following:

> “When you connect with an application or website it will have access to General Information about you. The term General Information includes your and your friend’s names, profile pictures, gender, user IDs, connections, and any content shared using the Everyone privacy setting. ... The default privacy setting for certain types of information you post on Facebook is set to “everyone.” ... Because it takes two to connect, your privacy settings only control who can see the connection on your profile page. If you are uncomfortable with the connection being publicly available, you should consider removing (or not making) the connection.” (McLuhan)

The quotes directly from Facebook policy in 2005 and today display the overall evolution of Facebook privacy policy. In-between the two statements

subsequent versions were present and altered since the original in 2005. As Opsahl described in his critical review of the ever changing Facebook policy and the mistreatment of users, “the policies tell a story when viewed together.” Facebook gained its core users by guaranteeing privacy to make those using it feel like “The Facebook” as it was called, kept the data users are not comfortable sharing, private. However, as Facebook gained more users and grew both financially and as a cooperation, it could have chosen to stay with its original ideology keeping Facebook protected and each user in control of their page. Unfortunately the administrators chose to help themselves and the company, along with its business partners by slowly removing control. (Opshal) Therefore, Facebook actively and effectively weaned their users off of what they expected to be a private environment and while doing so redefined what “private” means on this popular social networking website. The following Section discusses in detail research that has been done regarding what can happen on social media websites due to lax security polices that have be altered and held over the people active on the website.

3.1.3 Social Media Public Data

Extensive research has been completed with regard to the type of vulnerabilities users are susceptible to when signing up and using social media web services such as Facebook. The Privacy Rights Organization has taken each aspect of social media as a whole and broken down what is done on the foreground of the website and what happens in the background in regard to your sensitive data. According to their research, two types of public information

sharing exist, both are just as equally as incriminating and important to understand. (Pipes)

The user information that is popular to share on Facebook is photos, videos, age, gender and biographical information which can be your education, employment, hometown and location. Most users also, through other applications and “likes” share contacts, interests and friends. “Social networks themselves do not necessarily guarantee the security of information that has been uploaded to a profile, even when those posts are set to be private.” (Opshal) According to research it was demonstrated in May of 2012 unauthorized users were able to see private chat logs posted in public on their Facebook page. They continued to explain that while bugs are quickly fixed there is great potential to take advantage of the information leaked.

The second kind of public information is data which is gathered. In the case of Facebook, your location, profile and your networks are always visible. However, it also has the ability to track viewing of pages, store information associated with specific websites and track movement from one site to another. This in the end allows social media to build a profile around any user. (Opshal)

Building a profile happens very often on Facebook as most users now have mobile devices with the popular network application happily linked to their smart phone. Linking Facebook enables Facebook to not only track your location, but because it is on your phone allows access to contacts and the pages you visit through the application itself. This “profile” enables anyone that wants to find you

to do so with little or no effort. Referring to a precious point this personal identifiable information can be easily sold out and or leaked from third parties that have access to your information in accordance with the Facebook agreement. (Krishnamurthy)

3.1.4 Pubic Tracking Data: Possible Outcome

Based on the above information and that which is defined as public knowledge on Facebook today, a wide array of security and privacy concerns arise especially when discussing Personal Identifiable Information. (PII) This information is defined as “data which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." (Krishnamurthy)

The availability of this PII is outstanding and described in detail by Craig Wills and Balachander Krishnamurthy. They explain that on Social Media such as Facebook, PII is, but not limited to gender, birthday, age or birth year, schools, employer, friends and interests. Furthermore they tabulated data based on the availability of this information on different profiles using different Social Websites and the outcome was astounding. More than 70% of PII is available on media such as Facebook and by default is now public knowledge.

3.1.5 Pubic Tracking Data: Leakage Study

The theory that Wills and Krishnamurthy studied recently was tested and concrete proof was found that PII leakage on social media websites occurs. In order to test it, it is necessary to have the application “Live HTTP Headers” which is a Firefox extension and the ability to freely browse a Facebook profile. The extension displays HTTP request and response frames for all objects thus allowing the user to see what and to whom information is being sent. The findings of this study showed a “Leakage of PII.” Four types of PII leakage were found; transmission of the website Identifier to third parties, transmission of this identifier to applications, transmission of visited pages to third party servers as well as the linking of PII within and across the social media site.

“The possession of this identifier allows a third-party to gain much PII information about a OSN (Online Social Network) user to join with the third-party profile information about a user's activity on non-OSN sites. Analyzing the request headers we obtain via the Live HTTP Headers extension, we find that the OSN indenter is transmitted to a third-party in at least three ways: the Referrer header, the Request-URI, or a cookie. Note that accesses to third-party servers are often triggered without explicit action (e.g., clicking on an advertisement) on the user's part.” (Krishnamurthy)

3.1.6 Pubic Profile Information

Regardless of the background of data tracking, users still have quite a bit of control with regard to the actual information that they post on their personal

Facebook page. If users are to control the amount of PID uploaded not only will background tracking and third party app vulnerabilities be limited, but the following security concerns as they relate to human interaction, and visible access to PID on public profiles. Each of the following implications have been studied and reviewed by Privacy Rights Organization regarding real consequences that can take place based on the information users share on their profile

3.1.7 Who Has Access

As mentioned above, advertisers and developers collect personal information, then using the data profile each user to more directly influence them with products and services. The more direct threat however, are those who have direct access to your page such as identity thieves who seek out PID and other online criminals such as phishing or scam artists. The most concerning are people who seek out individuals based on their PID to intentionally harass and intimidate.

The Freedom of Information Act sheds light on how the government uses Facebook during many kinds of investigations. All government agencies and the US Justice Department have trained employees how to utilize Facebook not only for prosecutors in a court case but during security background checks. (Pipes) Facebook, as stated in their privacy policy are more than supportive with any requests by the US Government requesting information about a Facebook page regardless of the privacy settings.

Most people do not think about their online identity while applying for an apartment to rent, starting a relationship, a new job or applying for scholarships. Nevertheless, according to research the Facebook profile is often what people turn to in order to scope out the character of a person to understand someone who is starting to interact in a new environment.

3.1.8 Negative Affects: Lack of Privacy and Fraud

Facebook pages have been known to cause termination from employment and also have forced employers to not hire an individual based solely on the information they discover on a Facebook page such as a profile picture or gender. Profiling someone, as ironic as it is, has become very common and employers even have policies outlining what employees can and cannot post on their own Facebook pages. (Pipes) Negative side effects of social networking come in other forms than the obvious already discussed topics. Privacy Rights Organization also outlined and studied other common security concerns that can occur based on what is on a Facebook profile.

The most shocking of all is the use of a public profile for identity theft. If one actually takes the time to think about the information on Facebook, it can be very easy to steal an identity. As discussed, Facebook has your network, birthday, name and profile pictures which are forcibly public. According to the research by Allessandro Acquisti, based on the public information, your social security number can be calculated based on your birthday and the network a user is attached to; this is typically the hometown high school or college network. The prediction of such can be done with 98% accuracy and has been proven to

be true due to the national algorithm which is based on the birthday of an individual along with the persons birth town. (Acquisti) Furthermore, Facebook is full of people that have fake profiles and it has been known that the fake users try to use social engineering to mimic one of your friends in order to gain access to personal data. These accounts can be new or hijacked and using many methods such as phishing, misleading solicitations and generic data mining a friend request can be sent. The unfortunate truth is once the “Friend Request” from the fake account has been accepted access to all of your Facebook and its containing information has been granted.

On top of all of the problems that are most of the time apparent to the end user, sometimes developers write malware for the Facebook platform to collect more personal information such as passwords and usernames. While this would be terrible to happen to your page specifically, it also can affect you even if a friend of yours has had their Facebook page compromised. These rouge programs have the potential to collect unauthorized information from each person on the infected friend list.

3.1.9 Facebook Policy: Concerning Facts

Due to the affects and implications studied, it is important to understand what Facebook holds themselves accountable for and what users are actually signing up for. To follow, is a list of excerpts from the current Facebook policy following a quick explanation what can happen based on the Facebook policy. Each of the following can be found directly from the Facebook Privacy Page. (*Facebook)*

> "For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License)."

Facebook, as per its policy has exclusive rights to each and every piece of data, which is uploaded to its servers. This includes pictures, videos, posts and artwork that users choose to share. The question is where can these pictures potentially end up? Facebook reserves its right to use a picture on its servers on a national Ad. This could lead to a picture of yours used in some sort of derogatory advertisement based on what you post online. This information is now the property of (for lack of a better term) the Internet.

> "Your name, profile pictures, cover photos, gender, networks, username and User ID are treated just like information you choose to make public."

Most people do not think twice about what this short sentence means when it comes to their privacy. It is probably because they do not know what can be derived based on the information that Facebook is making public by default. Your networks, which often are your high school, allow people to derive your birthplace. That along with your profile pictures people can learn birthdays from the picture at the party or the "birthday" posting on the top of your page. Most people have their birthday documented or have a picture of the event as their profile picture. The picture in accordance with the timestamp, allows birth dates to be found regardless if they are directly posted or not. The most concerning part of this is the fact that all can be used to derive your social security number based on the national algorithm which is based on a mix of where you are born

(often close to your high school) and your birth date. The last four digits are literally everywhere and public knowledge. Matching the two sets of a data together a Social Security Number with 98% accuracy can be derived.

> “We only provide data to our advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it is no longer associated with you.”

Advertising partners have access to everything that is set to public as well as all that your friends make public about you such as Posts, pictures, likes, tags and location. Using this common information, companies can use a simple algorithm to narrow down your name even though “personal information” is stripped. Your location data is saved as well as posts and tags and if you are tagged at a location and with a friend it is simple to obtain who you are by deducing your friend and where you live. That along with your posts makes it very easy especially when tagging locations and people is very common on Facebook.

> “When we use the phrase "public information" (which we sometimes refer to as "Everyone information"), we mean the information you choose to make public, as well as information that is always publicly available.”

A quick Google search contains all of your posts, likes and pictures, This is all that needs to be done to access personal information even if you left this sensitive data public for a few minutes Google has them cached for months leaving pictures and posts vulnerable for all to see. This is potentially implicating because once it is cached with Google even after deleting from Facebook

anyone, such as employers only need to search your name to find posts or pictures that you thought were deleted.

> "Deactivating your account puts your account on hold. Other users will no longer see your timeline, but we do not delete any of your information. Deactivating an account is the same as you telling us not to delete any information because you might want to reactivate your account at some point in the future. You can deactivate your account on your account settings page. Your friends will still see you listed in their list of friends while your account is deactivated."

Even if deactivated, the account, your picture and name is still present on Facebook. Employers who do not like your "mutual friends," or people trying to "get ahead" of you can still use the data attached to your name even while deactivated. As discussed above the way employer's use Facebook is completely up to them and additionally it is hard to prove any illegal activity based on biases found on your Facebook page or connections to it. When deactivated, while the profile is not active, your "Friends" still have you linked to their page. Searching for your name on their list still will return a result.

> "When you delete an account, it is permanently deleted from Facebook. It typically takes about one month to delete an account, but some information may remain in backup copies and logs for up to 90 days. You should only delete your account if you are sure you never want to reactivate it."

Even after deletion, law enforcement or subpoenas can be issued to gain access to data. This is especially true for current background investigations as investigators search Facebook, posts and friends for this reason Facebook keeps a back log of about six months.

> "If you tag someone, that person and their friends can see your story no matter what audience you selected. The same is true when you approve a tag someone else adds to your story."

Each and every person that you tag has access to the piece of information in which they are tagged in. Not only the person you tag but each and every one of their friends do as well. This is based on their privacy settings not yours. An example how this can affect a user lies in a simple picture upload. If you upload a picture that may be incriminating or not “Employer Safe” and tag a friend in it, regardless of your privacy settings, if their settings are public this picture now can be seen by the entire world. One example, is a post that Joe made after being upset with Apple Store Geniuses. He writes, “Joe Lipari might walk into an Apple store on Fifth Avenue with an Armalite AR-10 gas powered semi-automatic weapon and pump round after round into one of those smug, fruity little concierges.” Within 45 minutes the SWAT team bashed down his door and arrested him. After a two-year investigation and trial, he was relieved but not after much cost and hassle. His “Friends” reported him. (Motal)

> “Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social. For example, one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list - which includes your User ID - so the application knows which of her friends is also using it.”

Third party applications are given your data which includes posts and likes everyday without your knowledge. Where it goes from there is unknown as Facebook removed all legal obligation to said information.

> “If you post something using a social plugin (another website such as news) and you do not see a sharing icon, you should assume that story is Public. For example, if you post a comment through a

> Facebook comment plugin on a site, your story is Public and everyone, including the website, can see your story. We receive data when you visit a site with a social plugin. We keep this data for a maximum of 90 days"

Typing your opinion about a political view or a news story could very well land you answering for it in a future court case as lawyers are known to use Facebook posts to support their case. All posts on such a place are public, and completely admissible in court. Local plugins most of the time are not on Facebook but directly found on websites that in fact link to Facebook servers. Furthermore, websites that you visit are not only logged with the site you go to but if Facebook is embedded in the site, Facebook has location and usage data on their systems. This information inevitably leaks to third parties through apps and eventually you could have ads and "likes" being associated with you that you did not condone.

> "As described in this policy, we may share your information when we have removed from it anything that personally identifies you or combined it with other information so that it no longer personally identifies you. We use information we receive, including the information you provide at registration or add to your account or timeline, to deliver ads and to make them more relevant to you. This includes all of the things you share and do on Facebook, such as the Pages you like or key words from your stories, and the things we infer from your use of Facebook."

"Liked" pages can be pulled down and given to virtually anyone. If you "like" a company, which is a competitor of your workplace, you may face some repercussions from your boss and possibly removal. Some employees have seen suspension time for liking a comment on Facebook. (Motal)

Methodology

4.1.1 Introduction

This section will describe in detail the route chosen to conduct my in depth research and study of Facebook users. The goal of my research again, was to find through user responses, and an interactive survey if education with appropriate real world examples and relating policies will allow for a better understanding of user actions followed by the possible repercussions of them while using Facebook. As it stands, the feeling of invincibility and carelessness is intertwined within people that use Facebook. I hope to discover if parts of Facebook policy, supported by with real world examples, will encourage users to reevaluate how Facebook is used and or gain a deeper respect and fear of the technology as a whole. This as apposed to dry user policies, should modify users thought processes while using the social media tool and create, in the end, a safer more secure user experience.

4.1.2 Research Method

In order to have an appropriate view and correct understanding of what questions to ask Facebook users in order to prove or disprove my hypothesis, a complete understanding of the inter workings of the website was required. Extensive research and review of the operations and the usage of Facebook was completed and furthermore because the survey was based on the knowledge of Facebook Security, much data had to be gathered regarding Facebook's current security policy and user agreements. Once the information was reviewed, a

series of selected excerpts of the policy were chosen. Using a cross sectional survey, those being questioned were given a series of qualifying questions to identify their validity in the subject.

There of course are many people using Facebook and those subjects are all different. They vary as it relates to their technical background, age, region, and their exposure to general security knowledge. Focusing my research on the Rochester Institute of Technology campus where there is a wide variety of age, ethnicity and background would limit my scope to a manageable number of participants while gaining the right amount of variant in each response. Current college age students are now known to be full Digital Natives and should have a basic knowledge of computing technology. In order to understand if my hypothesis was true a variety of sections are quite necessary to include in the survey. These sections distinguish each participant without gathering PID protecting them, while allowing my study to be thorough and well explained.

4.1.3 Survey Layout

The survey consisted of four main sections each gathering important factors relating to my focus of study. The first portion labeled “personal” gathers the participant’s year lever, major, home state or country, age, and gender. I opted to include this part as I thought would be interesting to know if age, year level or different regions of the world affect the way participants answer Facebook related sections of the survey. Age was added as I am only focused on college students at the Rochester Institute of Technology so if anything over the

age of 28 was answered the data was considered an outlier and not used in my study.

In order to gauge difference between each of the subjects responses who have different technical background, questions were added to understand users proficiency in both Facebook and technology overall. Starting the section off with a question that asks the user to gauge their proficiency in computers tells me some important information. First it let me know how much they use the computer, as someone who does not use one often will not answer “very proficient.” This it let me know if the subject is overall comfortable using the technology. A follow up to that question was asking the participant how often they use social networking, their level of knowledge of online privacy and if Facebook is their social media website of choice. This was very useful in determining if the user in fact uses Facebook, how much they know about it and if they consider themselves proficient. If a subject were to answer “no” to using Facebook their responses were discarded as my study was on people who use Facebook as a primary means of social communication. Finally, in closing to his portion, a few questions asked details about a subjects overall feeling of privacy while using the website. The best way to gauge a users understanding of Facebook was to ask their overall feeling of how secure the site is as it relates to their data. Learning the subject’s view of how secure Facebook is with their data was essential, as I needed to analyze an overall before and after picture user assumption of privacy as it relates to Facebook. Starting by asking them if they did in fact read the policy while signing up I was able to compare and contrast the

submissions based on if they read it the first time and they changed their opinion after my survey or, if they did not and still changed their view. Following he subjects view gauged their proficiency of Facebook based on the following definitions:

> **Facebook Expert:** You are on Facebook all the time know what every function of Facebook is and how it works. Furthermore you have read the Facebook Security Policy and User End Agreement and understand what each section means.
>
> **Facebook Beginner:** You use Facebook and understand posting, commenting and tagging however, you are not familiar with the details of how it works and you have not read the Facebook User End Agreements.
>
> **Do not Use Facebook:** You have never used Facebook and/or you do not know how to post, comment or tag.

Participants answered based on the definitions and I was able to compare and contrast the data based on the reaction section at the end section of the survey. If a user for example, is by definition a “Facebook Expert” and he or she decides after my survey to not use it as much, it can be considered a positive reaction and a confirmation of my hypothesis. However, if a subject feels they are a “Facebook Beginner” and still opt to use Facebook the same way even after learning of all its vulnerabilities my hypothesis would not stand true. This question in accordance with asking participants how secure they think information is on Facebook on a scale of 1-9, I was able to understand their thoughts behind how their data is managed and secured. 1 being the least secure and 9 being the most, subjects, before learning about all the incriminating activity answered based on their current knowledge.

The next section asked if a user participated in specific actions on Facebook. User activity was carefully defined in accordance with the policy findings in the current Facebook Policy and taken because I and other researchers found them to be potentially incriminating to the users data and future. Participants answered a question based on common actions preformed on Facebook. Then the Policy that relates to it was displayed along with an example of the potentially incriminating or un-secure reality. This showed the users, through an example, what could happen rather than simply telling them the policy. This method was chosen as users already have access to the policy however, they do not understand them, or do not read the important documents. Using this method, both styles of learning were used which focused on the facts and supporting data making a better impression on the person taking it.

Finally, the reaction section which being the most important part of the study portrayed the actual learning achieved. Leading with “Now that you know more about what is behind the policies of Facebook, please answer the following questions related to what you learned and your reaction to them.” The user answered in accordance with what they have learned. A simple question, asking if they will be more conscientious about Facebook activity allows the user to think overall if they have learned something significant starting a behavior modification thought process. Following that, the user was asked more specific questions that relate to the facts presented. All are important, however, the most important question of this section asked “How secure do you think you and your information on Facebook is on a scale of 1-9” once again this allowed a numeric gauge of

user responses based on the difference from the first time they answered to the last time placing a number on user thoughts.

4.1.4 Survey Software

Due to information security being a very important aspect of any data collection and research, the Survey software selected for my study was RITs own Clipboard located at “clipboard.rit.edu.” The survey was run and administered on the Clipboard server while being overseen by RIT facility. This not only ensured accuracy but also kept the human data being collected on RIT systems preventing any unauthorized loss of information. Subjects were able to login to the system and interact with the site. Upon completion of the survey they could submit their responses. Each of the entries were recorded and automatically saved into an excel spreadsheet for research and data analysis only.

4.1.5 The Process

The Rochester Institute of Technology has many means of communication and ways to interact and gather data. Fortunately, it was quite simple to find subjects simply by word of mouth or personal contacts. The goal was to reach upwards of 500 people and have at least a response of 100 subjects. The goal was reached and a subject pool of 110 people was met and used.

Once the subject was made aware of the research either by word of mouth, email or ironically Facebook. The link forwarded them to the Clipboard page where they were given the opportunity to login. This login process was simply to ensure they subjects were RIT students in order to keep the scope of my research in tact. Once in, they were able to see the agreement and the

overview of my research. Finally, after about a ten-minute process subjects submitted their responses thanking them for their input. As for the data analysis, the overseeing faculty removed all PID before my analysis was completed.

4.1.6 Completion

The research was complete when the analysis of the respondents proved or disproved the hypothesis. Students at the Rochester Institute of Technology, when presented with Facebook policy along with supporting evidence and policy facts will realize that Facebook is not as secure as previously assumed and change their activity accordingly.

Survey Results and Analysis

5.1.1 Overview

The following documents how secure respondents feel that Facebook is before and after completing the educational portion of the survey. As discussed, there are four sections to the survey which asked different questions collecting a wide set of variables. This section breaks down each variable that could affect the subjects responses and documents them into tables followed by a comparison of a “before education” and “after education” result. The “education” refers to the portion of the survey, which provided incriminating Facebook problems and actions supported by the privacy policy to the subjects. By analyzing the data, a true or false result in regards to the hypothesis can be made based on the responses to the survey. Based on their answers, one can conclude if the knowledge provided to the subjects was an effective method as stated in my hypothesis.

5.2.1 Demographic Information

A base demographic was important for this survey and study, the following gives perspective to who the subjects are in the study. Table 1 below displays the number of respondents in comparison to their gender.

Table 1 - Respondent Gender

Gender	Female	Male	**Number of Students**
Total	29	81	**110**

At the Rochester Institute of Technology the male to female ratio is 70/30. As displayed, the ratio holds about the same at a 73% male to 27% female respondent rate.

Furthermore, of the respondents, a majority was from New York State totaling at 51 and a variety of other states were included as well. As summarized below in Table 2, top ranking states are Connecticut and New Jersey with six, Pennsylvania with five and California, Maryland and Massachusetts totaling with four respondents. Initially, before surveying subjects, data favoring New York State was expected as the Rochester Institute of Technology is located in Rochester NY.

Table 2 - Respondent Home Location

Total Number of Respondents from Specific Location

Permanent Residence	**Number of Students**
California	4
Canada	2
Connecticut	6
Florida	2
Georgia	1
Hawaii	2
India	2
Maine	1
Maryland	4
Massachusetts	4
Michigan	1
Missouri	1
New Hampshire	1
New Jersey	6
New York	51
North Carolina	1
Ohio	2

Pennsylvania	5
Singapore	1
Texas	1
Vermont	1
Vietnam	1
Virginia	1
Wisconsin	1
Total	**108**

While RIT has enrolled approximately the same number of students in each respective year level, of the collected data, more students who are in their freshman to senior years at the Institution completed the questionnaire. Fifth year students totaled the least number of replies with thirteen participants and following the oldest of students, third year participants with a mere seventeen. A majority of subjects were in their fourth year or second year of study at RIT and choosing to include year level brought an understanding if more education at RIT affects student's thought of overall Facebook security.

Table 3 - Student Year Level

Total Number of Students for Each Year Level

Year Level	Number of Students
1st	21
2nd	31
3rd	17
4th	28
5th	13
Total	**110**

Breaking down the respondents and the major they each belong to, there was no surprise that a majority of subjects are of technical origin. Out of the 110,

twenty-eight are in an engineering field, fifteen in computing arts, and computer security there are thirteen. The remaining majors and number of replies are clearly documented in Table 4 below. The data shows at least a few people from each of the colleges on RIT campus permitting analysis of student Facebook security perspective from a wider group of RIT community members.

Table 4 - Student Major

Total number of students enrolled in enrolled in a specific major

Student Major	**Number of Students**
Arts	9
Business	12
Computer Security	13
Computing - Arts	15
Computing – Networking	7
Engineering	28
Information Technology	4
Languages	6
Mathematics	2
Multidisciplinary Studies	5
Sciences	9
Grand Total	**110**

The following portrays and briefly explains the respondent's answers to the "before education" questions in the survey. This includes each respondent and the self-evaluation of their technical skill, Facebook proficiency, Facebook use frequency, and a scale, which asks the respondents how they feel Facebook handles their data.

5.3.1 Before Facebook Education

Results from this segment of the survey are significant as it is the baseline for each of the set criteria planned to be analyzed once the “after education” is compiled and reviewed. The demographic information included are the students year, major and gender in order to gain an understanding of the amount of influence the survey had achieved. However, other baselines were added such as technical proficiency and Facebook use.

5.3.2 Year and Scale

Below Table 5 portrays the year level of the respondent in conjunction with the one – nine Facebook security scale. (one being least and nine being most)

Table 5 - Scale Vs. Year

Average interpretation of how secure Facebook is on a scale of 1-9 by students in each year level

Year / Scale	1	2	3	4	5	Average
1	1	1	1	1	0	1
2	0	2	2	2	0	2
3	3	3	3	3	3	3
4	4	4	4	4	0	4
5	5	5	5	5	5	5
6	6	6	6	6	6	6
7	7	7	7	7	7	7
8	8	8	8	8	8	8
9	0	0	0	0	0	0
Average	**5.48**	**4.26**	**5.41**	**4.71**	**6.38**	**5.04**

As documented, each year level has their own view regarding the security of Facebook. Based on the “security average” row it seems that first year students feel that Facebook is moderately secure, scoring a mean of 5.47/9. Fifth year students on the other hand feel that on average the website is more secure with their data scoring a 6.38/9. This could be due to the fact that the website has been used for a longer period of time by the fifth year students than the first year students thus creating a increased natural feeling of trust as previously discussed.

5.3.3 Frequency and Scale

In conjunction with the year level, asking the subjects how often they used the site allowed a clearer picture regarding how using Facebook more frequently affects trust and use of the site.

Table 6 - Scale Vs. Use Frequency

Average interpretation of how secure Facebook is on a scale of 1-9 by the frequency of use

Frequency / Scale	Few Times a Week	Never	Once a Day	Once Every Hour	Average
1	0	0	1	1	1
2	2	0	2	2	2
3	3	3	3	3	3
4	0	0	4	4	4
5	0	0	5	5	5
6	0	0	6	6	6
7	7	0	7	7	7
8	0	0	8	8	8
9	0	0	0	0	0
Average	**3.75**	**3**	**4.64**	**5.25**	**5.04**

As previously examined, using a piece of technology more often generates trust in humans and the results of the survey do not contradict previous research. Table 6 displays the frequency at which users are on Facebook against how much they trust the service. Respondents who never used the site before do not feel Facebook is very secure as they scored a mean result of 3/9. Trust of the website increases in accordance with the frequency. When Facebook is used a few times a week a 3.75/9 score was achieved followed by using it once a day with 4.64/9. The highest score was from the respondent's who use the popular social media outlet a "few times an hour" resulting in a 5.4/9 security rating.

5.3.4 Major and Scale

One expects the major of each student surveyed to have an affect to how the security of Facebook on the scale would be answered. Depicted in Table 8 below shows the breakdown of majors against how secure the respondents felt Facebook is with their data.

Table 7 - Scale Vs. Major

Average interpretation of how secure Facebook is on a scale of 1-9 by students in different majors

Scale / Year	1	2	3	4	5	6	7	8	Average
Arts	0	0	3	4	5	6	7	8	5.22
Business	1	0	3	4	5	6	7	8	5.33
Computer Security	1	2	3	0	5	6	7	8	4.00
Computing - Arts	1	2	3	4	5	6	7	8	4.87
Computing - Networking	0	0	3	4	5	6	7	8	5.57
Engineering	1	2	3	4	5	6	7	8	5.14
Information Technology	0	2	3	0	0	6	0	8	4.75
Languages	1	2	0	4	0	6	0	0	4.17
Mathematics	0	0	0	0	0	6	0	0	6.00
Multidisciplinary Studies	0	0	0	0	0	6	7	0	6.60
Sciences	1	0	0	4	5	6	7	0	5.11
Average	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**5.04**

Somewhat different results were found than expected based on the average response for each major. Scoring a 4/9 average, computer security majors thought before being educated that Facebook is least secure. The respondents who felt Facebook is most secure are in the Mathematics and Multidisciplinary Studies programs. This could be due to the fact that little to no

computing education is included in their program. However, the rest of the data proves to yield a small difference.

5.3.5 Gender and Scale

Table 8 - Scale Vs. Gender

Average interpretation of how secure Facebook is on a scale of 1-9 by gender

Gender / Scale	Female	Male	Average
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7
8	8	8	8
Average	**5.62**	**4.83**	**5.04**

In the initial analysis of gender, the subjects' major seemed to play a role in the results because females are not typically involved with computing majors at RIT. Referring to the Table 7 once again technical majors feel that the website is more secure. However, after reviewing the data, significant error could have been introduced into the results as the exact male to female ratio within each major overall at RIT is not known. Females seem to think Facebook is more secure. In order to analyze Female responses the data compared is the Frequency of Use of the networking site and gender on Table 9.

Table 9 - Frequency of Use Based on Gender

Frequency of use of Facebook differentiated based on the gender of students.

Frequency / Gender	**Few Times a Week**	**Never**	**Once a Day**	**Once Every Hour**	**Grand Total**
Female	3	0	5	21	29
Male	1	1	20	59	81
Total	**4**	**1**	**25**	**80**	**110**

However, interestingly enough as shown in the table above, usage does not influence how secure male and females think Facebook is. This is determined as the total number of males and females that took the survey is 81 and 29 respectively. Therefore, initially, in order to prove that females think Facebook is more secure based on usage, females must use it more than males. However, when placing the male to female usage into percentages based on the number of respondents that selected “once every hour” and the total number males and females it was found that 72% of males and females use Facebook at least once every hour. This concludes that regardless of usage, females feel it is more secure. Unfortunately, this is not part of my study; nevertheless, usage and trust of Facebook based on gender would be something worth researching in the future.

5.4.1 After Facebook Education

"After Education" is defined as the portion of the survey the respondents answered after reading through the Facebook vulnerability's and understanding what is behind the policies that the social media website has in place.

5.4.2 Year and Scale

Table 10 - Scale Vs. Policy Understanding

Average interpretation of how secure Facebook is on a scale of 1-9 by student year level after understanding Facebook policies.

Year / Scale	1	2	3	4	5	Average
1	1	1	1	1	0	1
2	0	2	0	2	2	2
3	3	3	3	3	3	3
4	4	4	4	4	4	4
5	5	5	5	5	5	5
6	6	6	6	6	6	6
7	7	7	7	7	7	7
8	8	8	8	0	0	8
Average	**4.62**	**3.48**	**4.53**	**4.18**	**4.69**	**4.18**

After reading, and hopefully understanding what Facebook and other people have the potential to do with personal data, online users seem to think that Facebook is at an average of 4.18/9 in regards to how secure the popular website is. As depicted in Table 10 there is not a significant difference when it comes to the year of the respondent as it relates to their opinion of Facebook security. Overall, it seems educating the respondents had a bit of an effect in

regard to the year level of the student. This is especially prevalent in fifth year students as they now feel the website has a similar security level as first years.

5.4.3 Frequency and Scale

Table 11 - Scale Vs. Policy Understanding (After Education)

Average interpretation of how secure Facebook is on a scale of 1-9 by the frequency of use after understanding Facebook policies

Frequency / Scale	Few Times a Week	Never	Once a Day	Once Every Hour	Average
1	1	0	1	1	1
2	2	0	2	2	2
3	3	3	3	3	3
4	0	0	4	4	4
5	0	0	5	5	5
6	0	0	6	6	6
7	0	0	7	7	7
8	0	0	8	8	8
Average	**1.75**	**3**	**3.88**	**4.41**	**4.18**

Respondents who use Facebook more often still have the most faith and trust in Facebook. Scoring a 4.4/9 “once every hour” comes out on top of the respondents. It is interesting to observe the way people interact with their data online even though they are introduced with incriminating evidence. The more you use something the more trust is invested in the technology.

5.4.4 Major and Scale

Table 12 - Scale Vs. Major (After Education)

Average interpretation of how secure Facebook is on a scale of 1-9 by major after understanding Facebook policies

Major \ Scale	1	2	3	4	5	6	7	8	Average
Arts	1	2	0	4	0	6	0	8	4.778
Business	1	2	3	4	5	6	7	8	4.583
Computer Security	1	2	3	4	0	6	0	0	2.846
Computing - Arts	1	2	0	4	5	6	7	8	4.667
Computing - Networking	1	2	3	4	0	0	7	0	3.429
Engineering	1	2	3	4	5	6	7	8	4.321
Information Technology	0	2	3	0	5	6	0	0	4.000
Languages	1	0	3	4	0	6	7	0	3.667
Mathematics	0	0	3	0	0	0	0	0	3.000
Multidisciplinary Studies	0	0	0	0	5	6	7	0	6.200
Sciences	1	0	3	0	5	0	7	0	3.889
Average	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**4.182**

While education seemed to tighten the gap between majors the multidisciplinary studies seems to not have changed their opinion much at all. Still ranging at 6.2/9 these students still are not affected. However, others like computing security and networking seem to feel that Facebook is a bit less secure than previously assumed.

5.4.5 Gender and Scale

Table 13 - Scale Vs. Gender (After Education)

Average interpretation of how secure Facebook is on a scale of 1-9 by gender after understanding Facebook policies

Gender / Scale	Female	Male	Average
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7
8	8	8	8
Average	**4.48**	**4.07**	**4.18**

Finally the respondents' gender as it relates to the scaled seemed to, after completing the educational portion of the survey, overall decrease. However, females still trust the website more than males and even after learning about the implications the difference between before and after is minimal compared to males.

5.5.1 Data Comparison

Finally, after analyzing separately the two sets of data "before education" and "after education" for the survey comparing both scenarios is important in order to gain a clear understanding regarding the subjects and their future actions. Student year levels, major, gender and Facebook use frequency were compared to the scale both before and after the respondent read and answered questions about the Facebook policies and possible vulnerabilities it presents to

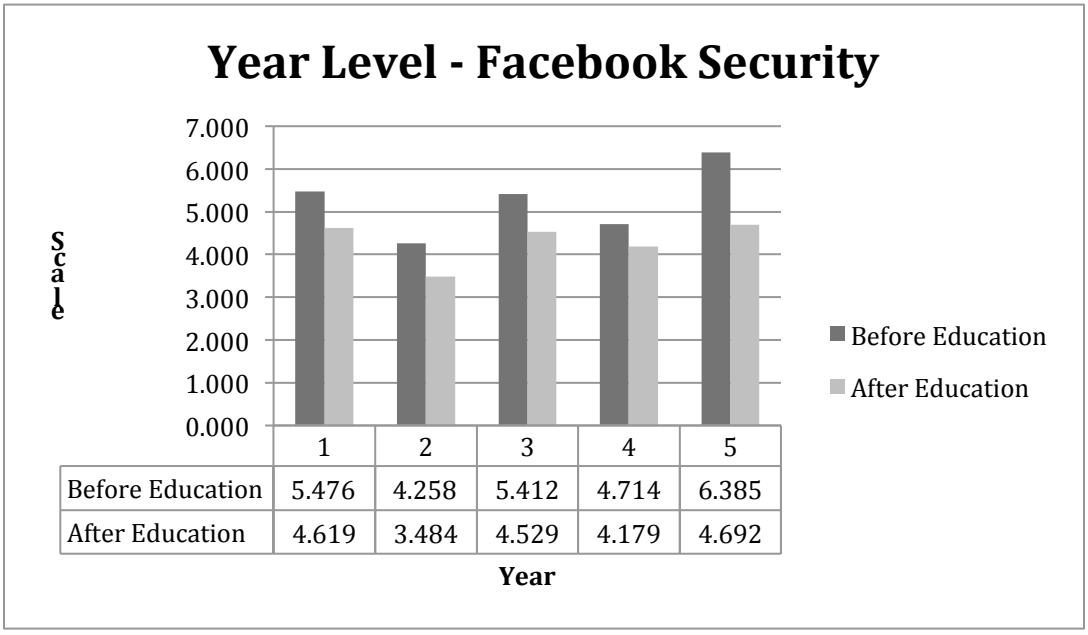
the users. Thought-provoking results were yielded and will be analyzed in this section.

5.5.2 Year and Scale Comparison

Initially, a student's year in the Rochester Institute of Technology was thought to have a possible effect on the way that the subject was to view the security of Facebook. After analyzing Figure 1, other scenarios can be explained along with the initial assumption.

Figure 1 - Comparison of Year Level and Facebook Security

Comparison of the average response on the security scale (1-9) for student year level both before and after understanding Facebook policies



	1	2	3	4	5
Before Education	5.476	4.258	5.412	4.714	6.385
After Education	4.619	3.484	4.529	4.179	4.692

As depicted in the bar graph above there was a slight effect to the subjects in different year levels when provided the education portion of the

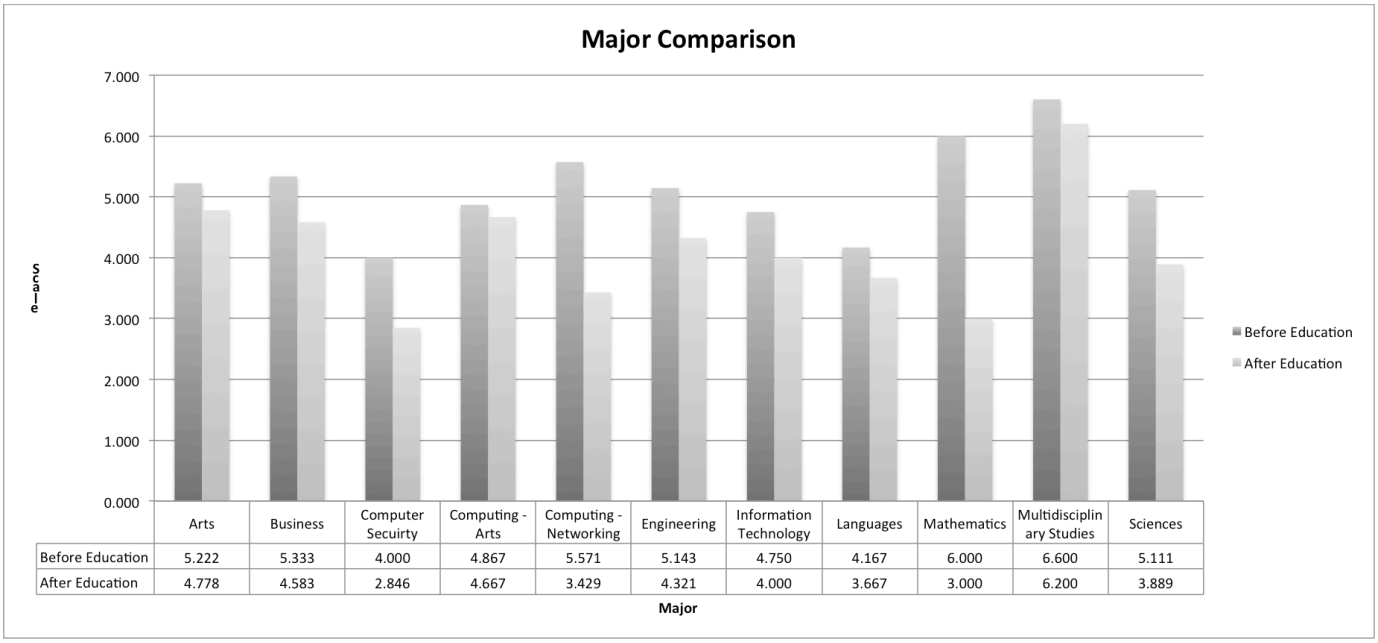
survey. Notably, the change seems to be similar for each of the independent groups for both the before and after responses. Note the first and second year responses: It seems incoming freshman and the first year students feel Facebook is more secure than second years. This most likely is due to the fact that they were exposed to basic knowledge of computing standards in their first year of their college experience. This undoubtedly resulted in the slight drop of faith in the website for their second year because students recently were exposed to the potential issues. Unfortunately, after the second year, faith in the websites ability to protect information steadily inclines. By the fifth year at the institution, respondents feel that the website is the most secure scoring a 6.38/9. On the contrary, after taking the survey the same people in their fifth year lost the most trust in Facebook and other people's ability to keep their information online safe. The education seemed to affect the users perspective about the website but minimally for first to fourth year students. Furthermore, fifth years had the most trust and similarly lost the most after being reminded of Facebook's flaws. It could be possible to remind those who forget how ensure the website is with just a bit of information. However, users are most likely to return to trusting the website after a period of time as diagramed between first and second year students.

5.5.3 Major and Scale Comparison

The survey not only overall reduced the trust that students have in the website but also produced interesting differences between student majors. It seems that different majors yield a dissimilar gap in trust that users have before and after learning about the security of Facebook.

Figure 2 - Comparison of Major and Security Scale

Comparison of the average response on the security scale (1-9) for students in various majors both before and after understanding Facebook policies



	Arts	Business	Computer Secuirty	Computing - Arts	Computing - Networking	Engineering	Information Technology	Languages	Mathematics	Multidisciplinary Studies	Sciences
Before Education	5.222	5.333	4.000	4.867	5.571	5.143	4.750	4.167	6.000	6.600	5.111
After Education	4.778	4.583	2.846	4.667	3.429	4.321	4.000	3.667	3.000	6.200	3.889

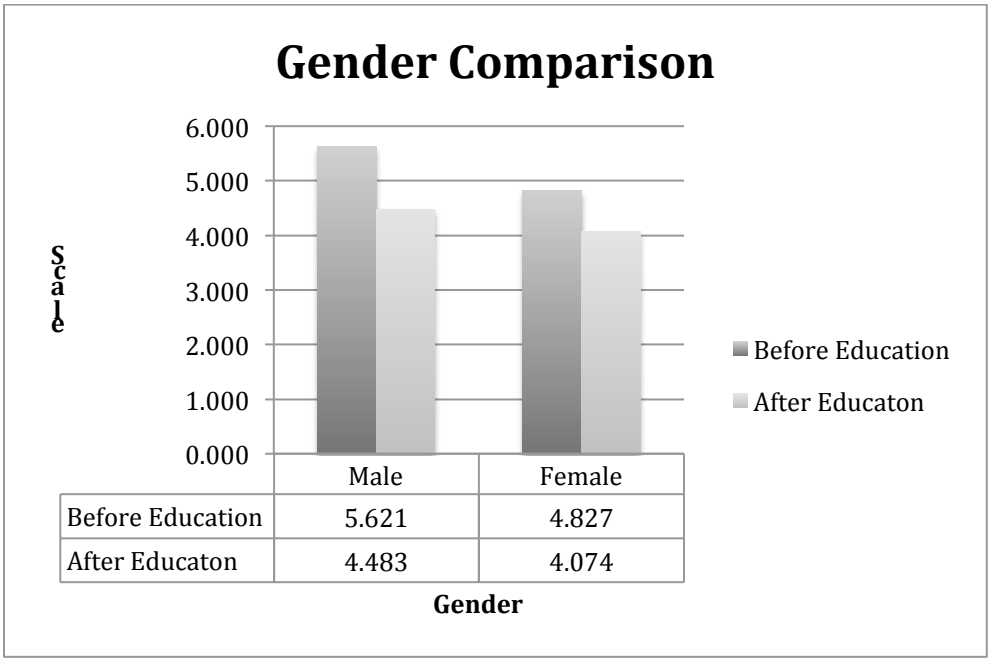
The respondents major had an impact on both their before and after view of Facebook security. Depicted above it seems that people without the proper professional background in computing and information technology are less affected by the information provided to them in the survey. In Figure 2 the difference in user perspective of Facebook security before and after is much

less with people who are in majors such as multidisciplinary studies and the arts. This is probably due to the fact that a different mindset is instilled in students who are in these majors. Art majors are focused on their line of work, while engineering, computing and business have to have a different set of knowledge and a different mindset in order to succeed in their programs. Mathematics resulted the biggest effect in regards to the before and after education scale. It could be due to the fact that math majors have faith in numbers and statistics, which results in a larger impact when presented with hard facts with supporting evidence. Computing majors on the other hand have a smaller mean margin as computing students are lectured about security all through their college career. While they may not have known about the details provided to them while taking the survey, they definitely have basic knowledge regarding the security of their data online. Therefore, while computing students have a larger margin than arts and multidisciplinary study students it was not as large as math students because of the prior knowledge and self trust these students have. “Self trust” refers to the fact they are in a computing major and feel they can handle anything that could happen with their data.

5.5.4 Major and Scale Comparison

Figure 3 - Comparison of Gender and the Security Scale

Comparison of the average response on the security scale (1-9) for student gender both before and after understanding Facebook policies



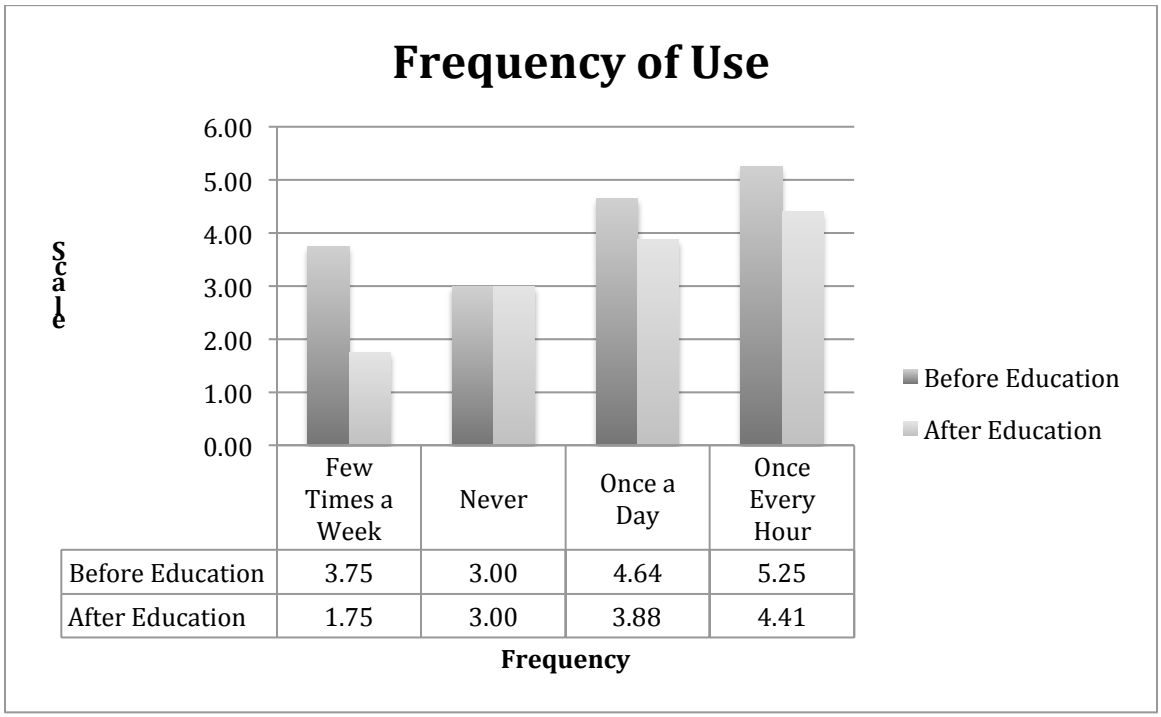
It has been said that we are influenced by our surroundings and what we are interested in. Therefore, the differences of male and female confidence in Facebook are not based on gender but that at which each is surrounded by more often which affects the overall results the gender yields. Males are more often in engineering and computing majors while females favor arts and business degrees at the Rochester Institute of Technology. Referring to the points above, males trusted Facebook more before the survey as they are typically in these majors and understand more implications before taking the survey. Females on the other hand still lost some faith but did not trust the site as much before the survey, reason being, initially they were not familiar with the information.

5.5.5 Frequency and Scale Comparison

Another point of explanation is the amount of time users are on the social media website. Figure 4 below shows the difference before and after in conjunction with how often subjects use Facebook.

Figure 4 - Comparison: Frequency of Use and Security Scale

Comparison of the average response on the security scale (1-9) for the frequency of use both before and after understanding Facebook policies



The main factor determined out of all of the different variables in regards to Facebook security and users perspective was the frequency in which subjects used the website. Both before and after, users who use the site more often trust in its security further. After learning about its risks, reduced trust the least out of each of the other four options. Expectedly, the people who do not use Facebook

did not have a changed opinion after learning about what can happen, however, those who use it rarely, in comparison to the majority, lost the most trust in the site losing 2 points on the scale. Subjects who use the site once a day or once an hour only dropped average of .79 points. All of the groups were subject to the same information but the data shows that the more users are logged in, the more they trust it or do not care about the possible implications

Final Findings

6.1.1 Overview

The final results, collected from the respondents, examination if they felt that Facebook is secure and if they still use Facebook the same way after learning the facts concerning their privacy. The results of this were a bit astounding. The respondents are persistent as they contradict themselves in regards to following the advice they, just a few moments before, learned.

6.2.1 Results

After the subjects were taken through the educational portion of the survey they were asked if they now felt that Facebook is a safe place to place their information on. Certainly, the data proves the previous assumption that respondents would feel Facebook is not a smart place for personal information after learning exactly what the policies allow people, the company, and other entities to do with the data users upload. Table 14 clearly shows that the subjects feel that the social media website is not keeping their data secure to their standards resulting in a data security approval rate of 25%. The other 75% feel that the website cannot manage their data and stop negative consequences from happening as per the “education” section of the survey.

Table 14 - Student Usage Change (After Understanding)

Number of students who will continue to Use Facebook after understanding Facebook policies

Usage change Options	No	Yes	Not Answered	Total
Total	2	81	1	**110**

Educating users to realize that Facebook is insecure is just one part of this study's hypothesis in which was examined. By asking the users if they would change their ways is the only definitive way to accurately know if the hypothesis was accurate. According to Table 15, seventy six percent of the subjects even after being shown the possible implications, policies and past cases say they will not change their behavior on Facebook. More positively, however, fourteen percent state they will limit their use on the website. Nevertheless, this does not define what the subject will limit as it could be time on the website or data restrictions. Furthermore, only eight percent say they will change their behavior to make their page more secure.

Table 15 - Students Use Will Use Facebook the Same

Students who will change their future usage of Facebook: Keep usage the same (yes), limit their use after understanding Facebook policies or discontinue use (no).

Options	Number of Students
Limit Use	16
No	9
Not Answered	1
Yes	84
Total	**110**

Out of the 110 subjects only a fraction were positively reacted to the survey by admitting a positive change in their behavior. Deeper philological behavior must be a factor in today's generation as it relates to the trust that they have in Facebook and other social media online.

Conclusion

It is interesting to find that students attending the Rochester Institute of Technology even after being provided with policy, supported by fact and examples still feel that Facebook is a secure and safe medium to share every aspect of their lives. This is in large is part due to the fact that Digital Natives are already used to the idea that their lives are online and anyone has access to the information. However, even after being made aware of the insecurities and admitting that this is not a safe place to be an active member on, the benefits of social connectivity seems to outweigh the security and benefit of restricting use of Facebook and other social media outlets. Times have changed from when Digital Immigrants were developing the very technology that the Natives trust in each and every day. This faith in technology has every reason to continue to develop and evolve as each generation uses and assimilates technology more and more into their lives. Unfortunately, college students at RIT feel that using Facebook is worth losing intimate details about their lives and risking the very future that they are trying to cultivate while attending the institution even after admitting to the website being less secure after learning about its problems.

Future Work

This study was directly interested in analyzing college students at the Rochester Institute of Technology and determining if they felt the benefit of being socially connected outweighed the current risks of using Facebook. These risks are, but not limited to, losing PID, potentially risking their future, creating interpersonal problems and potentially allowing a company to track users. It would however, be very beneficial to conduct this study over a longer period of time with either college students, or a larger group of individuals such as a set of students from freshman year of high school to senior year of college. This would allow an over-time assessment of their thoughts of the website capturing a broader view of the same hypothesis, capturing the trust time ratio more accurately. Furthermore, a wider, more in depth study of how each of the separate demographics affect the subject responses would benefit the overall policy study and human behavior of the newly established trust in social media. The demographics could be examined separately and researched with other common behavioral actions.

Works Cited

Acquisti, Alessandro, and Ralph Gross. "Predicting Social Security numbers from public data." *Proceedings of the National academy of sciences* 106.27 (2009): 10975-10980.

Böhme, Rainer, and Stefan Köpsell. "Trained to accept?: a field experiment on consent dialogs." *Proceedings of the 28th international conference on Human factors in computing systems*. ACM, 2010.

Business Dictionary. N.p., n.d. Web. 2 Mar. 2013. <http://www.businessdictionary.com/definition/ totalitarianism.html>.

Callis. Edmund. Berkeley, "Giant brains; or, Machines that think." (1955).

Engelberg, Elisabeth, and Lennart Sjöberg. "Internet use, social skills, and adjustment." *CyberPsychology & Behavior* 7.1 (2004): 41-47.

Facebook. Facebook, 11 Dec. 2012. Web. 21 Apr. 2013. <https://www.facebook.com/about/privacy>.

Google Support. Google, 2013. Web. 23 Mar. 2013. <http://support.google.com/websearch/answer/9016?hl=en>.

"Six Causes of Online Disinhibition." *PSY Blog*: n. page 2. <http://www.ncsl.org/issues-research/telecom/state-laws-related-to-internet-privacy.aspx>.

Hofman, Marcia. "EFF Posts Documents Detailing Law Enforcement Collection of Data From Social Media Sites." *Electronic Frontier Foundation*. Creative Commons, Mar. 2010. Web. 13 Apr. 2013. <https://www.eff.org/deeplinks/2010/03/eff-posts-documents-detailing-law-enforcement>.

Kanellos, Michael. "PCs: More than 1 billion served." *Cnet*. N.p., 30 June 2002. Web. 28 Apr. 2013. <http://news.cnet.com/2100-1040-940713.html>.

Kirkpatrick, Marshall. "Why Facebook is Wrong: Privacy Is Still Important." *Read Write*. Say Media, 11 Jan. 2010. Web. 10 Mar. 2013. <http://readwrite.com/2010/01/11/why_facebook_is_wrong_about_privacy>.

Krishnamurthy, Balachander, and Craig E. Wills. "On the leakage of personally identifiable information via online social networks." *Proceedings of the 2nd ACM workshop on Online social networks*. ACM, 2009.

McLuhan, Marshall. *Theories of Communication*. N.p.: Peter Lang, 2011. Print.

McMillan, Sally J., and Margaret Morrison. "Coming of age with the internet A qualitative exploration of how the internet has become an integral part of young people's lives." *New media & society* 8.1 (2006): 73-95.

Motal, Julious. "Charges Dropped Over Facebook Apple Rant." *PC Mag* 28 June 2011: n. pag. Print.

NSCL. National Conference of State Legislatures, 17 Apr. 2013. Web. 28 Apr. 2013.

Opshal, Kurt. "Facebook's Eroding Privacy Policy: A Timeline." *Electronic Frontier Foundation*. Creative Commons, 28 Apr. 2010. Web. 15 Apr. 2013.<https://www.eff.org/deeplinks/2010/04/facebook-timeline>.

Orwell, George. *1984*. N.p.: Signet Classic, 1950. Print.

Perlman, Leah, ed. "Facebook Ads." *Facebook.com*. Facebook, 6 Nov. 2007. Web. 21 Mar. 2013. <https://blog.facebook.com/blog.php?post=6972252130>.

Pipes, Sarah. "Social Networking Privacy: How to be Safe, Secure and Social." *Privacy Rights Clearinghouse*. Privacy Rights, Feb. 2013. Web. 9 Apr. 2013. <https://www.privacyrights.org/social-networking-privacy>.

Prensky, Marc. "Digital natives, digital immigrants part 1." On the horizon 9.5 (2001): 1-6.

Rice, Ronald. "Primary issues in Internet use: access, civic and community involvement, and social interaction and expression." *Handbook of new media: Social shaping and consequences of ICTs* (2002): 105-129. [10] Henderson, Samantha, and Michael Gilding. "'I've never clicked this much with anyone in my life': trust and hyperpersonal communication in online friendships." *New Media & Society* 6.4 (2004): 487-506.

Rideout, Victoria J., Elizabeth A. Vandewater, and Ellen A. Wartella. "Zero to six: electronic media in the lives of infants, toddlers and preschoolers." (2003).

Smith, Aaron, Lee Rainie, and Kathryn Zickuhr. "College students and technology." Washington, DC: Pew Internet and American Life Project. Retrieved 15 (2011): 12.

Suler, John. "The online disinhibition effect." *Cyberpsychology & behavior* 7.3 (2004): 321-326.

Appendices

A. IRB Approval Form

R·I·T

Rochester Institute of Technology

RIT Institutional Review Board for the
Protection of Human Subjects in Research
141 Lomb Memorial Drive
Rochester, New York 14623-5604
Phone: 585-475-7673
Fax: 585-475-7990
Email: hmfsrs@rit.edu

Form C
IRB Decision Form

TO: Richard Rockelmann; Harris Weisman

FROM: RIT Institutional Review Board

DATE: **April 8, 2013**

RE: **Decision of the RIT Institutional Review Board**

Project Title – Facebook Policy and Users Knowledge

The Institutional Review Board (IRB) has taken the following action on your project named above.

☒ Exempt 46.101 (b) (2)

Now that your project is approved, you may proceed as you described in the Form A.

You are required to submit to the IRB any:

- **Proposed** modifications and wait for approval before implementing them,
- Unanticipated risks, and
- Actual injury to human subjects.

Heather Foti, MPH
Associate Director
Office of Human Subjects Research

Revised 10-18-06

B. Survey

Facebook Security and User Knowledge

I would like to invite you to take part in a study to understand and enumerate the way users of Facebook interact with the website before and after understanding specific examples and background as to what can happen to a user based on Facebook's operational policy. This survey will take 5-10 minutes and will ask basic questions about you followed by inquiries about your use of Facebook. Examples of Facebook use will then be displayed following the policy that relates to it. You then will be asked to answer based on how you interact with the website. The last section will ask you what you learned and experienced in the previous section. These questions are the primary focus of the study.

This survey will not ask any personal information and I do not expect it to cause harm to the subject. The goal is to further extend the knowledge of Facebook users in order to keep them safe and secure by educating them about limiting the type of posts and data uploaded. Information accepted on this survey will be confidential as it is collected and kept within RIT computer systems using the "Clipboard" software which is overseen by RIT facility members.

This survey is completely voluntary and there will be no penalty if the subject chooses not to participate. Furthermore, the you may stop the survey at any time if you choose to do so.

If any concerns or comments arise please feel free to contact me, Richard Rockelmann at "rwr2640@rit.edu"

Personal Demographics - This section asks a bit of background information please answer as accurately as possible.

1. What year level are you at RIT?

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

2. What is your major?

3. What state or country (If international) are you from ?

4. What is your current age?

- 18-28
- 29-40
- 40+

5. Please select your gender:

- Male
- Female
- Other:

Technical Background - This section tries to gain an understanding concerning your technical background of both Facebook and technology as a whole

6. What is your technical proficiency with computers?

- Very Proficient
- Somewhat Proficient
- Not Very Proficient
- Not at All Proficient

7. How often do you use the internet for social networking

- Once Every Hour
- Once a Day
- Few Times a Week
- Never

8. What is your level of knowledge of your privacy and protection online?

- ○ Superior Knowledge
- ○ Average Knowledge
- ○ No Knowledge

9. Is Facebook your primary social networking website?

- ○ Yes
- ○ No

10. Did you read Facebook's terms of service before signing up for it?

- ○ Yes
- ○ No

Using the following definitions please answer the following questions:

FACEBOOK EXPERT: You are on Facebook all the time know what every function of Facebook is and how it works. Furthermore you have read the Facebook Security Policy and User End Agreement and understand what each section means. FACEBOOK BEGINNER: You use Facebook and understand posting, commenting and tagging however, you are not familiar with the details of how it works and you have not read the Facebook User End Agreements. DO NOT USE FACEBOOK: You have never used Facebook and/or you do not know how to post, comment or tag.

11. What is your level of Facebook Proficiency? (Please read the above definitions)

- ○ Facebook Expert
- ○ Facebook Beginner
- ○ Do Not Use Facebook

12.

Instructions: Please rate how secure your information on Facebook is: 1 being worst and 9 being best in terms of security

	1	2	3	4	5	6	7	8	9
On a scale of 1 – 9 how secure do you think you and your information on Facebook is	○	○	○	○	○	○	○	○	○

The next series of questions are specific to your type of activity on Facebook. After you answer a statement will appear showing a fact about Facebook relating to your specific type of Facebook activity as well as a quote from the Facebook privacy policy. Please not only answer the questions but read the information below them.

13. Do you have pictures and/or videos on Facebook that you hope to keep as your own?

- ○ Yes
- ○ No

FACEBOOK SECURITY TIP #1: Are you aware that you give Facebook explicit permission to use your "intellectual property" meaning information posted and uploaded becomes the property of Facebook. "For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission" ii. This gives Facebook exclusive rights to your information meaning they can (for free) use your pictures and videos in ads, promotions and they can even provide them to third parties. This image or video therefore is, for lack of a better term the property of "the internet" it can be placed virtually anywhere

14. Do you have your name on Facebook along with your Username, high school and or college "network" attached?

- ○ Yes

- No

FACEBOOK SECURITY TIP #2 Your name, profile picture, cover photo and your networks are defined as Public Information and this cannot be changed. Public information means ANYONE can access this information even those who do not belong to Facebook. ii. Derived personal information is knowledge that people can gather about you based on a few variables. Did you know that in order to figure out your social security number the only variables needed is your place of birth and your birthday? iii. Something to think about: Your "Networks" are often your home town high school or local city and your username is typically an email address used in many locations on the internet. Your birthday while not "public" people can figure it out using your posts or in this case your cover picture/profile picture of your most recent party celebrating your special day. iv. Once this information is gathered your Social Security Number can be derived to a 98% accuracy based on the national algorithm which is based on birthday and hometown. Think Twice!

15. How often do you "tag" someone in a picture or a post?

- Once a Week
- 3-5 Times a Week
- 10+ Times a Week
- Never

FACEBOOK SECURITY TIP #3 If you tag someone, that person and their friends can see your story no matter what audience you selected. The same is true when you approve a tag someone else adds to your story. ii. The fact is Facebook is designed for all to see as much as possible. Therefore what is posted on Facebook is most likely to be seen by not only your friends but your enemies as well. iii. Consider the following post "Joe Lipari might walk into an Apple store on Fifth Avenue with an Armalite AR-10 gas powered semi-automatic weapon and pump round after round into one of those smug, fruity little concierges." According to Joe it was a simple way to vent about his feelings concerning the apple store encounter he had that day. He was watching a movie that used this quote. He then posted it and changed it to his desired wording. Within the hour the S.W.A.T team was ramming down his door and arresting him. iv. The case took two years to be settled and thousands of dollars. v. Tagging is dangerous as someone reported him.

16. Do you "show" your friend list?

- Yes
- No

FACEBOOK SECURITY TIP #4 Are you aware that even though you may hide your friends list you are completely visible on your friends page who opt to show their friends publicly? ii. This makes it very easy to find who you know even though you think you are safe. By hiding your friends iii. Its very easy to fond out who you know and this can have negative implications especially when looking for a job or even a home loan. Who you know is everything and if someone feels you do not know the right people it may deem you unworthy for any kind of service or job you are opting to receive. iv. Additionally, If you make your profile not searchable, Facebook makes it convenient to find you again through the social people network called the "friends list" and mutual friends

17. Are you aware that any application, company and or website linked to Facebook is considered a third party? Any games and other applications that links to Facebook have their own rights to your data, at which point Facebook denies responsibly to your private data.

- Yes
- No

FACEBOOK SECURITY TIP #5 Most data that is sent and used for third parties are posts, likes and your friend list. Most of this data is randomized as Facebook states "As described in this policy, we may share your information when we have removed from it anything that personally identifies you or combined it with other information so that it no longer personally identifies you. We use the information we receive, including the information you provide at registration or add to your account or timeline, to deliver ads and to make them more relevant to you. This includes all of the things you share and do on Facebook, such as the Pages you like or key words from your stories, and the things we infer from your use of Facebook." ii. Deduction of information is easy even though your data is removed from personal information. Think about what you like and who you talk to. If you "Like" the ma and pa shop down the street it makes your location much easier to find. Your posts and your friends which are not hidden from your "personal information" makes it simple to narrow down who you are.. Just because your personal identifiers such as your Name, location and age are removed does not mean the third parties or any bad guys will have any problem finding out who you are

Reaction Section - Now that you know more about what is behind the policies of Facebook please answer the following questions related to what you learned and your reaction to them.

18. In the future are you going to be more conscientious about your Facebook activity?

- ○ Yes
- ○ No
- ○ Not Sure

19. What information in this survey surprised you the most?

20. Please check the following actions you might take:

- ☐ Remove Birthday
- ☐ Remove Hometown
- ☐ Remove third party Applications
- ☐ Remove Images or Videos
- ☐ Limit use of "likes"
- ☐ Limit Tagging
- ☐ Remove "friends" you do not know
- ☐ "Hide" friends list

21. Do you feel that Facebook is insecure?

- ○ Yes
- ○ No

22. Will you continue using Facebook the same way you always have?

- Yes
- No
- Limit Use

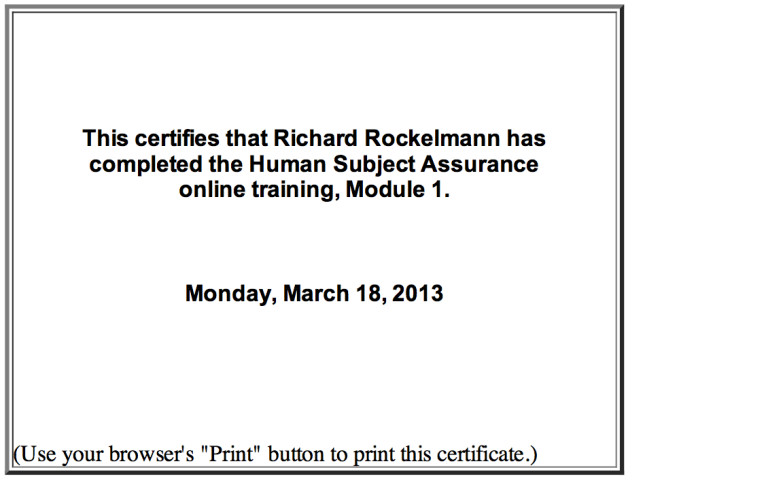
23.

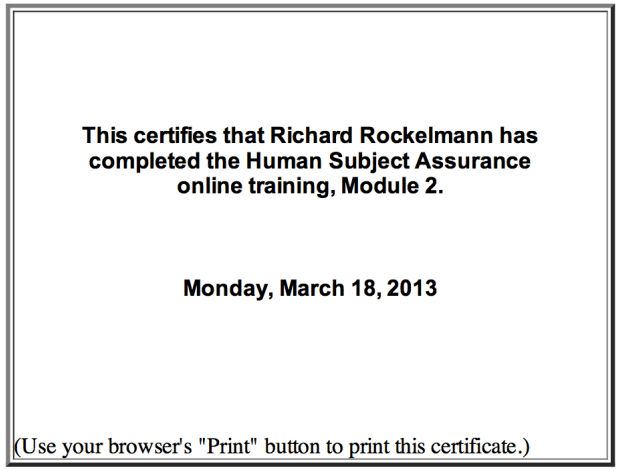
Instructions: After completing the above please rate how secure your information on Facebook is: 1 being worst and 9 being best in terms of security

	1	2	3	4	5	6	7	8	9
On a scale of 1 – 9 how secure do you think you and your information on Facebook is									

Please do not forget to press the "submit" button below!

C. Assurance Training





Human Subject Assurance Training

This certifies that Richard Rockelmann has completed the Human Subject Assurance online training, Module 3.

Monday, March 18, 2013

(Use your browser's "Print" button to print this certificate.)