INDIVIDUALS' PRIVACY CONCEPTIONS AND PERCEPTIONS: A TRANSLATION FROM PRIVACY IN GENERAL TO PRIVACY WITH GMAIL AND GOOGLE

by

Stephanie Jean Cleary

A thesis

submitted in partial fulfillment

of the requirements for the degree of

Master of Arts in Communication

Boise State University

August 2013

BOISE STATE UNIVERSITY GRADUATE COLLEGE

DEFENSE COMMITTEE AND FINAL READING APPROVALS

of the thesis submitted by

Stephanie Jean Cleary

Thesis Title: Individuals' privacy conceptions and perceptions: A translation from privacy in general to privacy with Gmail and Google

Date of Final Oral Examination: 24 April 2013

The following individuals read and discussed the thesis submitted by student Stephanie Jean Cleary, and they evaluated her presentation and response to questions during the final oral examination. They found that the student passed the final oral examination.

Julie Lane, Ph.D.	Chair, Supervisory Committee
Trevor Hall, Ph.D.	Member, Supervisory Committee
John McClellan, Ph.D.	Member, Supervisory Committee

The final reading approval of the thesis was granted by Julie Lane, Ph.D., Chair of the Supervisory Committee. The thesis was approved for the Graduate College by John R. Pelton, Ph.D., Dean of the Graduate College.

DEDICATION

I dedicate this graduate studies culmination to my parents. To my mother, thank you for your continual love, support, and best intentions. Your encouragement and resoluteness of my education instilled in me the values of hard work, persistence, and dedication necessary to accomplish this endeavor. To my step-father, thank you for your endless support, encouragement, and assistance in all of my pursuits, especially this one.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my family, friends, and loved ones for their support, encouragement, and help in this pursuit. I could not have accomplished this without you. Thank you.

I wish to give a special thank you to Dr. Julie Lane for serving as my sound board, guide, and adviser throughout this entire process. Your assistance in ensuring my vision and goals were accomplished while keeping this thesis focused through our discussions and edits is sincerely appreciated. Thank you to Dr. Trevor Hall for introducing me to the concept of communication, technology, and law through your instructions. Your insights have continually encouraged me to see an alternative perspective. To Dr. John McClellan, my deepest gratitude for constantly pushing me and my conceptions of communication and privacy. Your thought-provoking instructions and advice provided me the encouragement and determination to pursue this topic. Thank you to my committee for your support, dedication, and contributions to my education and thesis.

Last, but certainly not least, I would also like to extend a huge thank you to Patty Larimore for assistance in editing my thesis.

ABSTRACT

While privacy is not a new issue for Americans, the skyrocketing presence and use of technologies has altered existing notions and definitions of privacy. Although previous researchers have examined and tested privacy theories and privacy is currently being discussed by policy makers, privacy and rights advocacy groups, and online companies, individuals' perspectives on privacy remain unknown and unheard. Therefore, this study interviewed nine individuals' about their conceptions and perceptions of privacy in general and in the contexts of Gmail, Google, and Google, Inc. This study used inductive and deductive thematic analysis to identify and interpret patterns from participants' interview transcriptions and evaluate how the individuals think about, understand, and expect privacy. The findings of these privacy definitions indicated three contradictions in how the participants' conceptualize and perceive privacy: participants care about their privacy, but they aren't worried about it; privacy definitions and expectations differ depending on the context; and privacy policies are agreed to without being read.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

FTC	Federal Trade Commission
URL	Uniform Resource Locator (web address)
IP	Internet Protocol
EU	European Union

CHAPTER ONE: INTRODUCTION

Privacy in America goes back to the American Revolution when colonists felt their rights were being violated by Britain (World Digital Library, 2012). While time has progressed and life has inevitably changed, privacy concerns and issues still exist. The use of new technologies and the Internet has not only transformed traditional privacy concerns, but also amplified the issues regarding individuals' privacy with unprecedented conditions. The increase in technology over the years has created new privacy problems: images taken, conversations recorded, places accessed, and documents read without individuals' knowledge or permission. One technology in particular that is redefining the concept and magnifying concerns of privacy is the Internet as various online companies are collecting and compiling information on individuals such as purchases, hobbies and interests, websites visited, computer information and location, email address, credit card information, name, residence, phone number, etc.

While some of this information might not initially appear worrisome to Internet users, their information regarding "private" matters, e.g., emails and health related searches, is gathered along with information regarding "public" matters like social network status updates or blogs since nothing is private on the Internet. This can become a serious privacy concern and issue as information is continually collected and compiled by companies to create profiles of individuals. As more and more people use the Internet to accomplish everyday tasks and engage in online activities the severity of this matter

intensifies because online companies are collecting every bit of information associated with individuals and using that information to influence what users see from airline ticket prices to advertisements.

Concerned citizens, privacy watch groups, media outlets, and the Government have taken notice of these Internet privacy issues. The media and privacy groups discuss the current privacy concerns while also reporting on the Government's latest inquiries and investigations into online companies' practices regarding users' privacy[1]. Although there are multiple big online companies to consider when examining and discussing individuals' privacy, one company that has received an abundance of privacy related attention from privacy watch groups, media, and the government is Google, Inc. This attention can be attributed to Google, Inc.'s number one Internet search engine, Google, and one of the top three Internet email providers, Gmail, as email and search are the top two online activities (Purcell, 2011). Additionally, on average, an estimated 43% of global Internet users access Google's website, a percentage point or two ahead of Facebook, making Google the number one website visited by Internet users around the world (Alexa, n.d.). To put Google, Inc.'s ranking in perspective, their video website YouTube is the third most visited site with 32% of the world's online traffic, while Yahoo! comes in at fourth with around 20%, Wikipedia at sixth with about 11%, and Amazon at eighth with an estimated 9% of global online visits (Alexa, n.d.).

---

[1] Examples of issues regarding individuals' privacy with the technology company Google, Inc. include Bosker, 2012, "In Google's Privacy Settlement;" Kang, 2012, "Google Announces Privacy Changes;" Kang, 2012, "Group Sues, Accusing Google;" Swift, 2012, "Google's Moves Raise Questions;" The Associated Press, 2012, "Google to Include Gmail."

Whether or not Google, Inc. is aware of its number one standing among global Internet users, the company is undoubtedly aware of its users' demographics. Only about 13% of Google's global Internet users are in the U.S.A. so Google, Inc. has opened "more than 70 offices in more than 40 countries around the globe" to handle operations worldwide (Google, Inc., n.d., "Google Locations"). In addition, Google, Inc. provides 98% of the languages read by online users in its language translation service, Google Translate (Google, Inc., n.d., "Our History In Depth").

However, the privacy focused spotlight can also be ascribed to Google, Inc.'s recently changed privacy policy for the users of nearly all of their 100+ products. Despite ongoing user privacy incidents and the company motto "don't be evil," the announcement of the privacy policy change was made only five weeks before its implementation and without user or regulatory agreement. Furthermore, Google, Inc. demonstrated it does not consider users' privacy when former Chief Executive Officer (CEO) and current Executive Chairman Eric Schmidt said in an interview regarding users' privacy, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" (CNBC, 2009). While this argument could be seen as keeping with the company's "don't be evil" motto, it undermines the essence of privacy as something personal not shameful, embarrassing, or wrong. Schmidt's argument that nothing is private also suggests that Google, Inc. is not only aware of everything its users' are doing, but the company doesn't consider its big brother surveillance attitude an invasion or violation of users' privacy. Schmidt's and the company's disregard for users' privacy can also be seen in Google, Inc.'s renovated March 1, 2012, privacy policy as its implementation allows users' data to be shared across all of Google, Inc.'s products and

services (Helft, 2013). As Google, Inc.'s current CEO Larry Page stated, the privacy policy change would facilitate product innovation in that "virtually everything that [Google, Inc.] wants to do … is somewhat at odds with locking down all of [users'] information" (Cain Miller, 2012) to maintain their privacy. So when Page had to choose between the company's future new products and users' privacy, Page chose innovation and implemented a new privacy policy that would remove some of users' privacy protections to accomplish that.

Yet as with the privacy discussions among privacy watch groups, media, and the government, Larry Page and Google, Inc. have not asked the users' perspectives, opinions, or thoughts about their privacy. Given the global use of Google, Inc. products and services, the popularity of Gmail and Google among email and search users, and the company's renovated privacy policy on March 1, 2012, Google, Inc. will be the context for this study's examination of individuals' conceptions and perceptions of their privacy.

History of American Privacy

While privacy on the Internet is a recent issue, Americans' notion of an implied right to privacy originated from the Magna Carta in 13th century England (National Archives & Record Administration, n.d., "Magna Carta"). The Magna Carta was 63 articles of rights, liberties, and justices that wealthy Englishman decided to fight for when they were displeased with the king's rule (British Library, n.d., "Treasures In Full: Magna Carta"). While the Magna Carta did not explicitly state a right to privacy, the right to privacy has been implied from one of three enduring original clauses: "To no one will we sell, to no one deny or delay, right or justice" (British Library, n.d., "Treasures In Full: Magna Carta;" National Archives & Record Administration, n.d., "Magna Carta").

While the English government read this clause as a trial by jury during the 1300's, British barrister, judge and politician Sir Edward Coke interpreted it as an individual's right to liberty in the early 17th century (British Library, n.d., "Treasures In Full: Magna Carta"). Although the charter was initially written to guarantee peoples' rights, the charter and its articles would be revised and rewritten over the course of English history to maintain the explicit and implicit rights and liberties of the people.

So when Englishmen came over to the American colonies they brought with them the charters ensuring their liberties and rights (National Archives & Records Administration, n.d., "Bill of Rights;" National Archives & Record Administration, n.d., "Magna Carta"). When American colonists revolted against the King of England they were fighting for their rights, liberties, and justices created over 400 years earlier. After the colonists won the Revolutionary War those rights and liberties were put in the U.S. Constitution and the first ten amendments of the U.S. Bill of Rights to ensure Americans' freedoms in the future (Library of Congress, 2010; National Archives & Records Administration, n.d., "Bill of Rights"). While privacy was not the cause of the American Revolution nor made a law or an Amendment during the establishment of the United States of America, the notion of individuals' right to privacy has been implied from the explicit rights of individuals' liberties in the Bill of Rights: the First Amendment's protection of speech, religion, press, and people's assembly and petition to the Government; the protection of one's home in the Third and Fourth Amendments; the security of one's self, documents, and belongings "against unreasonable searches and seizures" in the Fourth Amendment; the Fifth Amendment's defense of an individual's "life, liberty, or property, without due process of law" and protection from "self-

incrimination;" and the Ninth Amendment's protection of the people's rights not explicitly stated in the Constitution (National Archives & Records Administration, n.d., "Bill of Rights;" National Archives & Record Administration, n.d., "Magna Carta;" Pember & Calvert, 2011; World Digital Library, 2012).

When Americans feel their privacy has been violated they seek restitution through the legal system and courts which have ruled that the right of privacy for the person and the home is implied in the Constitution and Bill of Rights (Henderson, 1999). While some of the first privacy lawsuits were won on the notion of privacy, it was former law partners Samuel D. Warren and future Supreme Court Justice Louis D. Brandeis' article "The Right to Privacy" (1890) that made a right to privacy a more prominent legal notion (Prosser, 1960, p. 384). Thirteen years later privacy finally become a legal statute with the *Roberson v. Rochester Folding Box Co.* (1902) case wherein Abigail Roberson's picture was used by Rochester on their flour packaging without her consent (Prosser, 1960). Although Roberson lost the case, public outcry for redress led to New York's first privacy law (Prosser, 1960). The *Roberson* case came up again three years later in *Pavesich v. New England Life Insurance Co.* (1905) where Pavesich's name and picture were used without consent (Prosser, 1960). The Georgia Supreme Court ignored the *Roberson* ruling rationale and set a new precedent in recognizing privacy as a right; however, the opposing decisions on privacy from these two cases led to a divide on privacy case rulings for the next 30 years (Prosser, 1960).

In *Olmstead v. U.S.* (1928), the Fourth Amendment's protection against unreasonable search and seizure was applied to wiretapping phone lines of Olmstead's house (Henderson, 1999). The Supreme Court ruled that the Fourth Amendment did not

apply because "nothing physical had been seized" and the house was not entered (Henderson, 1999, pp. 61-62). This ruling would stand until 1967 when the Supreme Court ruled in *Katz v. U.S* that a person could expect and has privacy in one's private activities (Henderson, 1999). The most important and foretelling impact of the *Olmstead* case was the dissenting opinion of Supreme Court Justice Brandeis', the same Brandeis who wrote "The Right to Privacy" with Warren 38 years prior. Brandeis argued that ways of invading privacy not conceivable by the founding fathers had emerged and the Constitution should be extended and applied to these new technologies or conditions (Henderson, 1999).

Americans' privacy has been shaped by their explicit and implicit legal rights, court decisions, and new communication technologies. While privacy is not a Constitutional or guaranteed right, it is an implied right the courts and justices have determined over time that needs to be extended to new technologies. In 1939 the public's desire and vehement demands for a legal expectation of privacy resulted in recognition of a right to privacy in the *Restatement of Torts*, The American Law Institute's publication of tort laws, and recognition by courts across the U.S. (Prosser, 1960). However, while individuals might desire and demand privacy there is no legal assurance that their privacy will be protected; just that they can seek reparations when the legal boundaries of their privacy have been violated. Former Supreme Court Justice Brandeis noticed individuals sought legal restitutions for violations of their privacy, as in the cases of *Roberson v. Rochester Folding Box Co.* (1902), *Pavesich v. New England Life Insurance Co.* (1905), and *Olmstead v. U.S.* (1928), but he also recognized the use of technologies in these cases to violate individuals' notions of privacy (Henderson, 1999). Hence Brandeis' foreboding

that privacy cases involving new technologies require legal decisions to serve as guidance for understanding individuals' privacy within these new circumstances. While former Supreme Court Justice Brandeis noticed the advancement and use of technologies to infringe upon individuals' privacy, he could not have anticipated the extent to which technology threatens individuals' privacy today, just as today's technological innovators and legal system cannot predict the privacy invasion situations individuals will face with future technologies.

Technological Influence on Privacy

The arrival and use of today's digital technologies such as satellites, GPS, cell and smart phones, the Internet, and email and search complicate Americans' understanding of privacy. Prior to digital technology, Americans understood privacy as an implied right that when violated could be resolved through the courts. The courts would then make rulings which would create legal boundaries on what constitutes individuals' privacy so everyone understood how they could expect privacy. However, as former Supreme Court Justice Brandeis noted, technology changes the expectations and violations of privacy which is why the Constitution should be extended and applied to these new technologies or conditions (Henderson, 1999). Yet the advancement of technology has occurred so quickly that the legal system has not kept pace with the new ways of invading privacy. And all the while, American culture has become more and more dependent on technology, evolving into a Technopoly (Postman, 1992).

As Postman's (1992) subtitle succinctly describes it, a Technopoly is the surrender of culture to technology wherein the technologies overrun culture by redefining everything, "what we mean by religion, by art, by family, by politics, by history, by truth,

by privacy, by intelligence" so that the new definitions meet the requirements of the technologies (p. 48). This redefinition of culture occurs because one new technology "changes everything" from "the things we think *about*" [original emphasis] and "the things we think *with*" [original emphasis] to "the arena in which thoughts develop" (Postman, 1992, pp. 18-20).

Privacy with digital technologies exemplifies the redefinition of how individuals' understand and expect privacy. Individuals used to be in control of what information companies and businesses had on them, but now digital technologies transmit information about the user to associated companies, sometimes without the user's knowledge. While satellites have allowed for the growth in wireless technologies, they also bring the concern of individuals being monitored without notification. Global positioning systems (GPS) contain transmitters that send out an individual's location via satellite signal to whoever is requesting or able to access it. Cell phone companies collect and retain customers' information including call and text logs and data and location information. In addition, every new cell phone has a GPS tracker installed for emergency purposes which can be turned on and monitored by cell phone companies, the account holder, those with a warrant or reasonable cause, and hackers.

The Internet has also redefined privacy while becoming a new source of privacy concerns and invasions for individuals as the number of Internet users with collected information multiplies. Identities and credit card information can be stolen. Individuals can post personal information and comments on websites which can sometimes never be removed. Emails and searches are stored on online companies' servers until the company deletes them. Companies collect every bit of users' information and put cookies, or

trackers, on computers to report back individuals' Internet activity information so companies can predict users' online behaviors and activity and compile and sell users' information (Lessig, 2006). As Henderson (1999) said, "the laws of economics in the information age say that information has value – it is a product that can be sold, just like socks, cars, and toothpaste" (p. 23). In 2000, Toysmart.com filed for bankruptcy and "placed a 'for sale' ad in the *Wall Street Journal* listing as assets is [*sic*] databases and customer lists," despite Toysmart's privacy policy that they would never share users' personal information with a third party (Regan, 2003). The personal information listed for sale included "names, addresses, credit card and phone numbers, and shopping preferences" (Regan, 2003, p. 14). More recently, Barnes and Noble acquired Borders in late 2011 including "Borders' customer loyalty list, which includes millions of names, emails addresses, physical addresses, phone numbers, and some purchase information" to gain customers' business (Bomey, 2011).

However, online companies' business practices regarding individuals' privacy are not limited to consumers, they affect users and website visitors as well. The Internet activities of email (electronic mail) and search are two popular reasons why individuals go on the Internet and "form the core of online communication and online information gathering, respectively. And they have done so for nearly a decade, even as new platforms, broadband and mobile devices continue to reshape the way Americans use the internet and web" (Purcell, 2011, p. 3). In 2012 the Pew Internet & American Life Project found that 91% of adults online were finding information on the Internet with search engines and 59% used search engines daily, making it the second highest online activity (Purcell, Brenner, & Rainie, 2012). The number one online activity was email with 92%

of adults using it, 61% of them on a daily basis (Purcell, 2011). While search and email may be the top two Internet activities they are also drastically reshaping and transforming the definitions and conceptions of individuals' privacy. Emails can be accessed and monitored by the company providing the email service, employers, those with a reasonable cause or warrant, and hackers. Emails can also be sent to others without the original sender's knowledge and kept as permanent records on computer servers, which are subject to the same privacy concerns as email accounts. The Internet searches individuals conduct are relevant to and provide information about them so search engine companies monitor and record these searches to gather users' information for advertising and profit making. While these email and search practices benefit online companies, they disregard users' privacy preferences.

The complexities of these current technologies exemplify how the technologies are redefining individuals' privacy. Instead of the U.S. courts or legislation attempting to define individuals' privacy with technologies, they have let the technology companies define what users' privacy is through privacy policies. Thus users' privacy on the Internet depends on how each online company defines it in the privacy policy. Consequently, it is difficult for individuals to contribute to the creation of privacy definitions since the technology companies are defining privacy without consideration of users' expectations. One online company that has recently demonstrated its authority to change the definition of users' privacy without their input is Google, Inc., a predominant provider of both email and search to Internet users.

Google, Inc.

Google, Inc. was founded in late 1998 with the sole product of their Internet search engine Google. In December 1998 Google was recognized for "an uncanny knack for returning extremely relevant results" and PC Magazine named it top search engine of 1998 (Google, Inc., n.d., "Our History In Depth"). By 2000 Google had become the "largest Internet search engine" with an index of one billion websites or Uniform Resource Locators (URLs), 15 different language options, and a search engine toolbar allowing its users to search the Internet without going to the Google webpage (Google, Inc., n.d., "Our History In Depth"). Today Google has an improved search algorithm, an index of over one trillion URLs and over one billion images, allows preview snapshots of websites, auto-completes search queries, and is available in more than 72 languages including Klingon and Swedish Chef (Google, Inc., n.d., "Our History In Depth"). In a 2012 survey of 2, 253 Americans, 83% of participants said they use Google most often for searching (Purcell et al., 2012). Even among Google, Inc. users Google remains the most popular product while Gmail is the second most popular (Alexa, n.d.; Mohan, 2012).

Initially, Gmail was used primarily as an internal email system. It was launched for public testing on April 1, 2004, and became available to everyone on February 14, 2007. (Google, Inc., n.d., "Our History In Depth;" Sullivan, 2004). Since the public release in 2004 Gmail has evolved to provide searching of emails, over 10 gigabytes of storage, grouping of emails into conversation threads, instant chat, phone calls, "a very significant spam detection system built in," secure encryption, access and use from anywhere including mobile devices, 40 interface languages, and is monetarily free

(Google, Inc., 2004; Google, Inc., n.d., "Our History In Depth;" Google, Inc., n.d., "Top 10 Reasons To Use Gmail;" Sullivan, 2004). Although "there are no uniform statistics" to compare the amount of users between email providers," Google, Inc. "claimed 350 million active [Gmail] users" in the January 2012 earnings call (Brownlow, 2012). This number tied Hotmail's October 2011 estimate of 350 million users and outranked Yahoo! Mail's October 2011 estimate of 310 million users (Brownlow, 2012). Despite the popularity of Gmail and Google, Google, Inc. has not always pleased individuals with the treatment of their privacy.

Privacy Incidents

Google, Inc.'s most recent privacy incident was the settlement of its StreetView privacy lawsuit with 37 states in March 2013 ("Google Settles StreetView Privacy Lawsuit," 2013). When taking pictures of streets between 2008 and 2010 for the street view feature of its Maps product, Google, Inc. also collected individuals' data from their unsecured wireless networks without their permission ("Google Settles StreetView Privacy Lawsuit," 2013). The collected data included information regarding Internet history, text messages, emails, passwords, and other confidential information (Guynn, 2013). The settlement agreement required Google, Inc. to disable or remove the equipment that collected the data from the street view vehicles, stop its collection of unauthorized data, destroy the data it did collect, train and educate Google, Inc. employees on consumer privacy data and issues, sponsor a public service campaign where individuals can learn how to secure their wireless networks, and pay $7 million in fines ("Google Settles StreetView Privacy Lawsuit," 2013; Guynn, 2013).

Previously, in August 2012, Google, Inc. agreed to pay "a $22.5 million fine for violating a consent decree [regarding users' privacy and control over collection of their personal information] signed with the Federal Trade Commission (FTC) and misrepresenting privacy settings to users of Apple's Safari browser" (Bosker, 2012) when they placed cookies on computers of Safari users after the users blocked tracking cookies (Bartz, 2012; "Google Will Pay $22.5 Million To Settle FTC Charges," 2012). However, Google, Inc. did not have to admit any wrongdoing and instead the company "repeatedly attributed issues to internal oversight or error" or "blamed the presence of Google advertising cookies on a 'functionality' in the Safari browser that activated them, adding that it 'didn't anticipate that this would happen'" (Bosker, 2012).

These incidents were not the first times Google, Inc. upset privacy concerned users, privacy advocacy and watch groups, and governments. Within the same week as the FTC ruling, Google, Inc. announced plans to include Gmail results in Google searches. Under this plan, when Gmail users are logged into their account and search with Google their emails will be displayed along with the Internet search results (The Associated Press, 2012). While this "feature" is still in the testing stage, privacy advocates are worried this may be a repeat of the "Buzz" disaster in 2010 (The Associated Press, 2012).

Buzz was a program created to provide updates of users' personal information and online activities to their most emailed contacts in Gmail, but in Google, Inc.'s attempt to keep up with other social networking sites Buzz was implemented without users' permission (Hill, 2010). The Buzz fiasco resulted in a class action lawsuit and allegations by the "FTC that Google used deceptive tactics and violated its own privacy promises to

consumers when it launched" Buzz (Swift, 2011). As a result, Google, Inc. paid $8.5 million to an Internet policy and privacy education fund to settle the class action lawsuit and agreed to adhere to FTC audits over the next 20 years, and improve users' privacy (Hill, 2010; Liedtke, 2012).

However, in March 2012 Google, Inc. consolidated 60 of their products' privacy policies into one privacy policy enabling the company to combine all the personal data from users' accounts across multiple products into one user account profile (Swift, 2012). This change prompted U.S. privacy advocacy group Electronic Privacy and Information Center (EPIC) to file a federal lawsuit for violating users' privacy and the June 2011 Buzz–FTC settlement terms that Google, Inc. must inform users of privacy policy changes and get users permission for those changes (Kang, 2012, "Group Sues, Accusing Google"). Furthermore, Google, Inc.'s new privacy policy did not solely affect U.S. users, but applied to all the Google, Inc. users around the world which triggered European Union (EU) Data Protection Authorities to investigate Google, Inc.'s new privacy policy ("Google Privacy Policy: Six European Data Protection Authorities," 2013). After the EU authorities' subsequent requests and efforts to have Google, Inc. attempt to meet the European Data Protection Directive requirements and Google, Inc.'s failure to do so, the authorities from France, Germany, Italy, Spain, the Netherlands, and the U.K. are pursuing legal enforcement actions ("Google Privacy Policy: Six European Data Protection Authorities," 2013).

While Google, Inc.'s privacy incidents over the last five years and the recent privacy policy overhaul that was unexpected and abrupt for a company with the motto "don't be evil," they reflect the company's priority on innovation over privacy. As the

current CEO expressed, the privacy policy needed to change in order "to create new products that know more about Google [Inc.] users" (Cain Miller, 2012).

The New Privacy Policy

On January 24, 2012, Google, Inc. publicly announced the privacy policy would be revised from the general policy set in place on October 20, 2011, and its hundreds of millions users would be notified via email and messages on its web pages, including the Gmail and Google home pages (Kang, 2012, "Google Announces Privacy Changes"; Whitten, 2012). The new main privacy policy replaced the 60 existing privacy policies for its products and services on March 1, 2012,[2] [3] and "explains what information we collect, and how we use it, in a much more readable way" (Whitten, 2012). Would anything change in the new privacy policy?

> The main change is for users with Google Accounts. Our new Privacy Policy makes clear that, if you're signed in, we may combine information you've provided from one service with information from other services. In short, we'll treat you as a single user across all our products, which will mean a simpler, more intuitive Google experience. (Whitten, 2012)

This "intuitive" experience means that searches provide suggestions and information based on users' emails and data, products and services are linked and

---

[2] Google, Inc. updated the March 1, 2012 privacy policy on July 27, 2012. The modification to the privacy policy was the addition of "Fiber," Google, Inc.'s broadband internet network, under the "Specific product practices" section. The language, contents and intent of the updated privacy policy did not otherwise change from the March 1, 2012 version.

[3] Google, Inc. updated the July 27, 2012 privacy policy on June 24, 2013. This change occurred after this study's interviews and analysis were completed. The modification to the privacy policy was the title change of "the Ads Preferences Manager" to "Ads Settings" under the "Transparency and Choice" section. The language, contents and intent of the updated privacy policy did not otherwise change from the March 1, 2012 version.

synchronized when a user is logged in, and advertisements are relevant to users' information (Whitten, 2012).

Are there any changes for non-account users? Those without a Google, Inc. account can still search with Google, watch videos on YouTube, get directions and location information from Maps, and do the same activities as before (Chavez, 2012). Non-account users will experience the same privacies granted to those with accounts except that information gathered from each product or service will not be associated with a Google, Inc. account. In other words, the information provided by a non-account holder while searching with Google and watching videos on YouTube will still be collected and cookies set like every other Google user, but that information will not be linked to and combined in a user account with personal information as it is with account holders. Instead, non-account users' information will be recorded into Google, Inc.'s system based on the computer's Internet Protocol (IP) address, any telephone information provided, or cookie information that identifies the user's browser or computer (Google, Inc., 2012, "Privacy Policy").

Why does all this information need to be collected and compiled? Google, Inc. states this information is "to provide, maintain, protect and improve [services], to develop new [products and services], to protect Google and users, offer tailored content – like more relevant search results and ads" (Google, Inc., 2012, "Privacy Policy"). While Google, Inc. also says information gathered from cookies, pixel tags, and other trackers are to improve the user's experience and its services, this collected information can include user's personal information (Google, Inc., 2012, "Privacy Policy").

Google, Inc. also stores and analyzes identifying data from search engine logs for 9 or 18 months (Google, Inc., n.d., "Privacy FAQ"). Google, Inc. says it stores search engine log data to improve the quality of search results, create more services, and "prevent against fraud and other abuses, like phishing, scripting attacks, and spam, including query click spam and ads click spam" (Google, Inc. n.d., "Privacy FAQ"). Google, Inc. states the search engine logs are not anonymized until 10 months for IP addresses and 19 months for cookies because this "strike[s] a reasonable balance between the competing pressures we face, such as the privacy of our users, the security of our systems and the need for innovation" (Google, Inc., n.d., "Privacy FAQ").

Google, Inc.'s privacy policy includes that they never sell or share any user's personal information with any entity outside of Google, Inc. except with domain administrators, for processing by external parties, legal reasons, or unless the user's consent is given (Google, Inc., 2012, "Privacy Policy"). In addition, Google, Inc. states that all of the collected information that is not personally identifying can be shared publicly and with Google, Inc. partners just like before (Google, Inc., 2012, "Privacy Policy").

The privacy policy also states it is not enforcing a "one account per person" policy, but "if you're signed in, we may combine information you've provided from one service with information from other services. In short, we'll treat you as a single user across all our products" (Whitten, 2012). So despite how many accounts a user has with Google, Inc. those accounts will be combined and not remain separate for each product or service.

So what if users do not like or agree with the changes in Google, Inc.'s new privacy policy? Google, Inc. states users can use their products and services how they choose to or elect to use a different service provider, but if users do decide to use any Google, Inc. product or service they are subject to the new privacy policy as there is no opt-out (Masiello, 2012, "Setting The Record Straight"; Whitten, 2012). Google, Inc. said it believes these changes make the privacy policy "simpler and more understandable" and "users' experience seamless and easy by allowing more sharing of information among products when users are signed into their Google Accounts" (Chavez, 2012). However do Google, Inc.'s privacy policy changes reflect individuals' privacy preferences and concerns?

Americans have known privacy as an implied right and have been able to seek redress for violations through the legal system, but the development of digital technologies has changed the ways Americans conceptualize and define privacy. Where individuals were previously able to affect the notion of their privacy, now online companies determine what individuals' privacy is through the company's privacy policy. In an attempt to reintroduce individuals' voices to the understanding of their privacy, this study will examine individuals' thoughts and beliefs about privacy, in general and with Gmail and Google, and establish whether or not their privacy perspectives coincide with Google, Inc.'s March 1, 2012, privacy policy.

CHAPTER TWO: LITERATURE REVIEW

What Is Privacy?

Alan Westin (1967) was one of the first scholars to investigate privacy and defined it as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7). The author also described privacy as four states necessary to the individual, "solitude, intimacy, anonymity, and reserve" (Westin, 1967, p. 31). Westin discussed the history of privacy and intrusions upon privacy before addressing tools for invading privacy, struggles for control of privacy, and the legal aspect of privacy in regards to technology.

Hollander (2001) examined the history of privacy and discussed "the language by which we designate, mention, describe, and invoke the (increasingly amorphous) concept of privacy" (pp. 5–6). Hollander claimed that "private" or "privacy" is a sense and "is much closer to 'personal' with regard to (a) property, (b) one's body – one's 'person' … thus touching on 'intimate' – and (c) something more like 'secret'" (pp. 6–7). Hollander's purpose was to acknowledge the individualistic, perceived nature of privacy despite the general social acceptance over time.

Contrastingly, Margulis (2003) looked at privacy in psychological and social research to discuss it from psychological, social, and behavioral perspectives. Definitions in social and psychological research were discussed before comparing the commonalities in Altman's (1975) theory of privacy through levels of social interaction and Westin's

(1967) theory of privacy functions and states to further understand privacy as a psychological and social issue and behavioral concept (Margulis, 2003, p. 245).

In an attempt to unify previous definitions of privacy, Tavani (2007) combined four previous definitional theories of "nonintrusion, seclusion, limitation, and control" to create a unified, comprehensive privacy theory, "the Restricted Access/Limited Control (RALC) theory of privacy" (p. 2). The RALC theory, an approved alteration of Moor's (1990, 1997) and Moor and Tavani's (2001) theories, compared "the *condition* of privacy" versus "a *right* to privacy" [original emphasis], "a *naturally private situation* and a *normatively private situation*" [original emphasis], and information control through consent, choice, and correction to determine an individual's privacy (Tavani, 2007, pp. 11–12).

Moore (2008) evaluated various definitions of privacy before suggesting and arguing for his own moral definition of a "'control'-based definition of privacy rights," where privacy right is determined by controlling who has access to oneself and his or her information (pp. 413–414). Moore claimed and defended that "a right to privacy can be understood as a right to maintain a certain level of control over the inner spheres of personal information and access to one's body, capacities, and powers" (p. 420) while recognizing the similarity of this definition to the RALC theory presented by Moor and Tavani (Moore, 2008, p. 428).

Ramsay (2010) discussed five concepts of privacy as individualistic needs and the importance of privacy as a right. Ramsay argued the most common, and thus first "sense," is information control and the remaining notions, in order, are "freedom from interference and observation," "the maintenance of a sphere of inviolability around each

person," "solitude," and "domesticity" (pp. 289–291). While the author acknowledged the legal arguments that could be made, the emphasis was on the morality and needs of these privacies by individuals in society.

Is Online Privacy A Concern?

In 1981, Louis Harris & Associates, Inc., with guidance from political and legal scholar Alan Westin, published a 1979 national survey addressing the public's opinion of privacy (i.e., Westin's definition of "collection, storage and use of personal information") (p. 4). The survey included the answers of 2,131 individuals to questions regarding "personal dimensions of privacy," "employee/employer relations," "privacy-intensive industries," "government and privacy," and "how to protect privacy" (Louis Harris & Associates, Inc. & Westin, 1981, p. 4). The general conclusion was that the public's concerns about these privacy areas had increased since the last Harris survey most likely because of an increase in technology, computer use, and "the collection of so-called 'personal data'" (Louis Harris & Associates, Inc. & Westin, 1981, p. 3). Almost ten years later, in 1990, Louis Harris & Associates, Inc. and Westin again explored the public's concerns of privacy and again found that privacy concerns had increased among the public with 70% of Americans concerned about threats to privacy (Louis Harris & Associates, Inc. & Westin, 1990, p. v).

So in 1995 when Louis Harris & Associates, Inc. and Westin again repeated the same procedure for a mid-decade study and again found that the majority of Americans were concerned about privacy, Westin decided to categorize Americans into three groups. The 25% of Americans that were most concerned about privacy were labeled "privacy fundamentalists," the 50% that were somewhat concerned about privacy were called

"privacy pragmatists," and the remaining 25% of Americans that were least concerned about privacy were known as "privacy unconcerned" (Louis Harris & Associates, Inc. & Westin, 1995, p. 13).

While Louis Harris & Associates, Inc. and Westin (1981, 1990, 1995) identified a growing public concern of personal information privacy and found three levels of privacy concerns amongst individuals, Sheehan (2002) questioned Westin's privacy groups and decided to replicate the Louis Harris & Associates, Inc. and Westin 1995 study to determine if the three levels of privacy concerns applied to online consumers. The results showed that 3% of participants were "alarmed" compared to Westin's 25% of fundamentalists, 81% were pragmatists compared to 50%, and 16% of participants were "unconcerned" compared to 25% in Westin's results (Sheehan, 2002, p. 27). Given the large group of pragmatists the researcher divided this group into two sub-groups: 43% of all the participants became known as "privacy wary" and 38% of the total participants were classified as "privacy circumspect" (Sheehan, 2002, p. 27). Thus the researcher had found that privacy fundamentalist, pragmatic, and unconcerned did not apply to online consumers and the more appropriate four labels to replace them were privacy alarmed, wary, circumspect, and unconcerned.

Online Privacy Concerns

Yao, Rice, and Wallis (2007) wanted to determine if online users' concerns of privacy were related to Internet experience, Internet diversity, belief in privacy rights, desire for privacy, concern in using the Internet and its associated risks, and gender. While the researchers found no correlation between gender and privacy concerns, their results "suggested that individuals' beliefs in privacy rights and the dispositional desire

for privacy in general are the main factors determining concerns about privacy issues in the specific context of the Internet" (Yao, Rice, & Wallis, 2007, p. 719). Thus, individuals with a greater desire for privacy and a belief in a right to privacy are more likely to be concerned about online privacy. However, the researchers did find that the desire and belief in privacy can be influenced by the other variables tested and believed that different individuals' privacy preferences may be an additional factor.

Milne and Rohm (2000) examined consumers' knowledge of information data collection and removal of personal information with businesses to determine consumers' privacy based on their ability to control their personal information. The researchers proposed that privacy only exists when the consumer is aware of data collection and the methods of name removal from databases, and if the consumer is not aware of those two variables in conjunction then the consumer does not have privacy. The researchers found that while over 95% of the respondents knew businesses they engaged with retained their name, address, and phone number, only 63.9% and 45.6% knew credit card information and purchase history information was retained, respectively (Milne & Rohm, 2000, p. 243). However, "only 45% [of the total respondents] were knowledgeable of name removal mechanisms" from company databases (Milne & Rohm, 2000, p. 244). Therefore the researchers concluded that only 34% of the total participants were aware of their data collection and able to remove their information and thus had privacy (Milne & Rohm, 2000, p. 244).

In an effort to determine individuals' willingness to provide information on the Internet, the Nielsen Company conducted a survey about privacy concerns, specifically "rights to privacy, data security, control over personal information, and confidentiality"

(Kachhi & Link, 2009, p. 75). The results suggested "an interesting paradox in the views and attitudes of internet users toward concerns about privacy and personal information:" While the majority of the respondents agree that they are worried about personal privacy, they feel they can't control how their personal information is used and that companies and the government know too much of their personal information, 80% of respondents stated they were comfortable making online transactions or purchases with secure websites (Kachhi & Link, 2009, p. 78).

Dinev and Hart (2004) looked at perceptions of vulnerability and ability to control information with perceptions of Internet privacy concerns. The privacy concerns, as determined by survey respondents, were the discovery and abuse of personal information, suggesting "that users associate privacy concerns based on information access and privacy concerns based on information abuse" (Dinev & Hart, 2004, p. 419). The authors believed this finding supported their belief that privacy is a separate construct from control and vulnerability, but "control, vulnerability, information privacy concerns and abuse privacy concerns are related and form a complex nomological net" (Dinev & Hart, 2004, p. 420).

Turow and Hennessey (2007) explored individuals' trust of institutions and Internet privacy of personal information and found that while the respondents were unsure if websites would protect or disclose their personal information, individuals still readily provided their personal information to websites. The suggested reason behind this contradictory behavior was that over 75% of respondents believed that laws or regulation would be somewhat to very effective in protecting respondents' information (Turow and Hennessey, 2007, p. 309). However, one quarter to one third of respondents were unsure

if legislation and regulation of businesses and government would protect or disclose their information (Turow and Hennessey, 2007, p. 309). The majority of participants were uncertain and neither trusted nor distrusted businesses and government, while the remaining respondents were divided between trusting and distrusting businesses and government (Turow and Hennessey, 2007, p. 309).

In analyzing these results, Turow and Hennessey (2007) found another contradiction. More "time online is related to the decreasing belief that institutional actors will help to protect personal information," but trust in the Internet, preference for regulation, and "having more self-reported skill also associates with the optimistic opinion that institutional actors will not disclose information without permission" (Turow and Hennessey, 2007, p. 314). So the more trust in the Internet, belief in the law, and greater skills and abilities one has, the more likely that person is to believe personal information will be protected. However, as soon as that individual becomes Internet savvy, the opposite belief of companies' disclosure of personal information becomes the predominant perspective. Thus, the researchers concluded that Internet users "simultaneously tend to voice two potentially contradictory beliefs: that major institutional actors will work to help them protect their personal information online, yet disclose information to other parties without internet users' permission or knowledge" (Turow and Hennessey, 2007, p. 315).

Miyazaki (2008) also looked at the question of consumers' trust and personal information privacy via website use, but with a focus on cookies. The first part of the study manipulated cookie disclosure and cookie use in a present-absent setting through a privacy statement and pop-up notification, respectively. The results showed that only in

the cookie use but no notification condition, "the implied social contract appeared to have been breached, which resulted in lower trust and usage-related intentions" by the participants (Miyazaki, 2008, p. 26). The second part of the study attempted to determine a "moderating role of desire for privacy on how cookie usage influences attitudes and intentions" (Miyazaki, 2008, p. 27). The study found that those with a greater desire for privacy had lower consumer trust, usage, and intentions than those with little preference for privacy. Additionally, the detection of cookies lowered trust, usage, and intention even more. While more experienced users had lower consumer trust and intentions than those with less online experience, the detection of cookies reversed this effect and those with less experience had lower consumer trust, usage, and intentions than more experienced users.

Joinson, Reips, Buchanan, and Schofield (2010) examined the relationships between online self-disclosure and privacy concerns, perceived privacy, privacy behaviors, and trust in two studies wherein privacy was considered privacy of personal information. The first survey tested privacy concerns and previous behaviors with self-disclosure, perceived privacy, and trust. The results indicated that participants' perception of privacy and previous privacy behaviors and concerns affected their self-disclosure, but trust was the strongest predictor of situational self-disclosure. Additionally, the relationship between perceived privacy, trust, and self-disclosure was stronger than the relationship between previous privacy behaviors and concerns, trust, and self-disclosure. The researchers suggested "that people's interpretation of the trustworthiness of an organization, or their perceived privacy in a specific context, are not influenced by their

general privacy disposition" but by "situational cues to make a decision rather than their preexisting attitudes" (Joinson, Reips, Buchanan, & Schofield, 2010, p. 18).

In their second study, Joinson et al. manipulated trust and privacy to determine the effects on trust, perceived privacy, and self-disclosure. In their survey, privacy was manipulated by either a strong or weak privacy policy and trust was manipulated by URL/domain names, institutional affiliations, proper spelling and grammar, and advertisements, with the high trust condition appearing as a legitimate university study. The results indicated that high and low trust led to greater disclosure, but only in strong privacy conditions. Low privacy and low trust was the sole condition to result in less self-disclosure. Therefore, as long as there is one high condition, either privacy or trust, self-disclosure will be the same as in a high privacy–high trust condition and "that the impact of privacy on behavior is *moderated* by trust, but that this moderation is not linear" [original emphasis] (Joinson et al., 2010, p. 17).

Meanwhile, Park (2011) investigated the role digital literacy plays in controlling personal information online through knowledge of the Internet, personal information privacy behaviors, and associations to Internet users' demographics. The study's results indicated that although most users understood collection and use of their personal information, an understanding of institutions' basic data practices and technical terminology was low. Given respondents' low levels of technical familiarity, users were less likely to engage in privacy enhancing technologies and more likely to control information by withdrawal, hiding, and avoidance. Therefore the researcher concluded "it is clear that generic technical familiarity functions as the most significant predictor of personal information control" (Park, 2011, p. 16).

Viseu, Clement, and Aspinall (2004) "explored the perceptions and practices of online privacy" (p. 93). They interviewed "lagging," i.e., "low income; low education; English as a second language; and seniors," Internet access users from age 20 to over 60 to see "if, and how, privacy concerns shape online experience and vice versa" (Viseu, Clement, & Aspinall, 2004, p. 95). The researchers did not give a definition of privacy so participants' meanings of privacy were vastly different. Although the researchers could not draw conclusions about their research at the time of publication, they found that the majority of participants thought privacy could be best maintained through selective disclosure of personal information and ownership of a computer as opposed to using a public computer, especially when banking or providing personally identifiable information. The reasons provided by the participants for these two predominant privacy preserving perspectives were not reading the privacy policy, lack of knowledge or resignation on protecting information, knowing and trusting the businesses interacted with and enjoying the personalization received, and nothing to fear or hide.

Best (2010) investigated "the contradiction between people's professed opinions and their actual behaviours" in screen technologies, focusing on surveillance claims of a "control society" with the aim of advancing "an understanding of whether and how users, or 'data subjects', actually consent to surveillance in their everyday lives" (Best, 2010, p. 7). The research suggested that "the majority of respondents were 'not bothered' about surveillance, or if they were aware of its dangers in a general sense did not feel themselves to be specifically at threat" (Best, 2010, p. 11). The participants' reasons for a disregard of surveillance included: "I'm not that important," "pretty small in life," "doesn't really affect me," being invaluable or undesirable, "not doing anything wrong,"

"nothing to hide," and unashamed of online behavior (Best, 2010, pp. 11–12). The researcher determined these reasons were founded from "a belief in the transparency and accuracy of information traces being amassed" (Best, 2010, pp. 11–12). Thus, respondents were "not bothered" about surveillance because of the belief that they were "unimportant" or "had nothing to hide," any collected information is correct and truthful, or information can be corrected to the truth or explained by the individual. However, 40% of the study's participants said they practiced evasion of information by "changing or altering information about themselves in online forms" or "giving out false or incomplete information in online forms" (Best, 2010, pp. 11–13).

Best also addressed consent and participatory surveillance with "loyalty programmes and credit cards, their completion of online forms, [and] their agreement to the terms and conditions of various sites" (Best, 2010, p. 17). The researcher found that respondents fall into one of three categories: "that surveillance is a worthwhile trade-off due to the need to balance care and control," "that it is a system of more immediate rewards and punishments," or "that it is an automatic process over which they have no control" (Best, 2010, pp. 17–19). However, individuals still expressed concern within each belief category. Although the smallest portion of participants believed in the trade-off, they still expressed the concern of when does monitoring people's web activities violate privacy? (Best, 2010, p. 18). Meanwhile, those in the rewards and punishments group "'take the good with the bad' to keep using the technology" because "it's not like signing your life away" when agreeing to online policies (Best, 2010, pp. 18–19). However, the majority of participants were in the "fatalistic" group where "there [isn't] any way to avoid it these days. This is just a feature of our times" (Best, 2010, p. 19). The

researcher concluded that “respondents are not simply unconcerned by surveillance, but perceive instead a lack of options at their disposal,” and questioned that “if the majority of users are faced with a trade-off that can be described as expedient at best and as inevitable at worst, can consent truly be said to exist?” (Best, 2010, pp. 20–21).

Search and Email Privacy Concerns

Search and email are two of the main reasons individuals go online with “roughly six in ten online adults engaging in each of these activities on a typical day” (Purcell, 2011, p. 3). So in 2012 the Pew Internet & American Life Project conducted a survey of search users “about whether they think it is okay for search engines to use information about them to rank their future search results” (Purcell et al., 2012, p. 18).

Eight hundred and twelve adult search users were asked about “a search engine keeping track of what you search for and then using that information to personalize your future search results” (Purcell et al., 2012, p. 19). Sixty five percent of respondents felt it was bad as the information provided may be limited, while 29% said it was good because search results are tailored (Purcell et al., 2012, p. 19). When asked this question differently, 73% of adult search users felt it was bad because it violated privacy and about 23% “would be okay with it, even if it means they are gathering information about you” (Purcell et al., 2012, p. 21). As for using that collected information, 59% of 1,729 online adults have “noticed advertisements online that are directly related to things you have recently searched for or sites you have recently visited” (Purcell et al., 2012, p. 22). When the search users were asked how they felt about these targeted advertisements online, 68% were opposed to having online activity tracked and analyzed while 28% were okay with seeing advertisements and information related to their interests (Purcell et

al., 2012, p. 23). So the Pew Internet & American Life Project decided to ask how many individuals know what is going on with their information online. Out of 1,729 online adults, only 38% are "aware of any ways internet users like yourself can limit how much personal information websites collect about you" (Purcell et al., 2012, p. 26). Of those 38%, 81% erased their Internet history, 75% utilized Web sites' privacy settings, and 65% altered their Internet browser privacy settings to limit collection of their personal information[4] (Purcell et al., 2012, p. 25).

Although the Pew Internet & American Life Project did not address email in their 2012 survey, this does not imply that users may not have privacy concerns with Gmail. Users' personal information in their account and emails are used for targeting certain advertisements to them. As Google, Inc. states, "our computers scan messages to get rid of spam and malware, as well as show ads that are relevant to you" (Masiello, 2012, "Busting Myths;" Markoff, 2004; Sullivan, 2004). However, that does not mean the analyses of users' email contents are not being stored and compiled into their account profile "to tailor individual advertising messages" when logged in and using Google, Inc. products or services (Masiello, 2012, "Busting Myths;" Markoff, 2004).

Unanswered Questions

These studies address various issues related to privacy: perspectives and theories of privacy, how much individuals are concerned about privacy, individuals' awareness and knowledge of privacy, how individuals strive for privacy, and individuals' privacy

[4] The Pew Research Center's Internet & American Life Project recognized "there are a range of other strategies that users can employ, including the deletion of cookies and the use of anonymyzing software and proxies that were not part of this survey" (Purcell et al., 2012, p. 25).

concerns with search and email. However, they leave unanswered some foundational privacy questions regarding individuals' privacy perspectives such as how individuals define privacy for themselves, in general and in the context of the Internet. Additionally, questions about individuals' privacy with the popular Internet activities of search and email have yet to be addressed. As these matters have not been answered, the users' voices are unknown, unheard, and unconsidered in privacy discussions. By asking these and similar questions of individuals, their privacy perspectives and behaviors can be understood, recognized and reintroduced into conversations and decisions about their privacy, especially in the context of the Internet. Therefore, the goal of this study is to understand individuals' conceptions and perceptions of privacy: how individuals define privacy, what individuals' privacy expectations are on the Internet, and if and how individuals' definitions and expectations of privacy translate from the offline to the online world. The research questions guiding this study are: How do individuals conceive of their privacy, generally speaking and with Gmail, Google, and Google, Inc.? and, How do individuals' privacy perceptions align or misalign with the reality of how Google, Inc. handles users' privacy according to the March 1, 2012 privacy policy?

CHAPTER THREE: METHODS

To accomplish this study's goals of how individuals define and expect privacy offline and with Google, Inc. online, and how those definitions and expectations translate to the reality of the online company's privacy policy, nine participants were interviewed and their responses were analyzed for themes. After identifying privacy themes, Google, Inc.'s March 1, 2012, privacy policy was examined to determine how Google, Inc. defines and handles its users' privacy. Finally, participants' privacy expectations and assumptions themes were used to analyze how Google, Inc. states they manage users' privacy to determine if participants agree with Google, Inc. on privacy.

Based on previous qualitative study and qualitative interview research discussions (Creswell, 2003; deMarrais, 2004; Denzin & Lincoln, 2002; Rubin & Rubin, 1995) the use of qualitative methods in this study allowed for an exploration of how the participants think about and experience privacy. Participants' used language they felt most accurately described their conceptions and perceptions which provided an opportunity for this researcher to learn and understand their meanings. Qualitative interviews allowed for broad questions to be asked initially and followed-up with specific questions based on participants' responses. This ensured participants discussed their thoughts using their own language, meanings, contexts, and definitions. In addition, participants' language use and meanings provided knowledge as to how they define, know, and experience privacy.

Participants

As this study includes individuals' perceptions of privacy with Gmail and Google, it was necessary that participants were Gmail and Google users. Since the emphasis and goals of this study are to gain information and insight on individuals' privacy conceptions and perceptions through their definitions and expectations, which have not been gathered by previous Internet privacy studies and will stimulate questions for future research, a representative sample is not necessary (Best, 2010; Viseu et al., 2004). As previous technology and privacy researchers have demonstrated, when a study focuses on a certain group of individuals, recruitment is accomplished in the best possible way to meet participant requirements (Best, 2010; Viseu et al., 2004).

Additionally, a representative sample of Gmail and Google users is not possible for this study as Google, Inc. does not provide any information about its users to the public (Google, Inc., 2012, "Privacy policy"). Therefore a snowball sample was used to recruit Gmail and Google users through the researcher's contacts in the Boise, Idaho area.

The characteristics required of qualifying participants were residence in the Boise area, English-speaking, between the ages of 18 and 65, and current use of Google or Gmail. These characteristics were developed so that interviews could be conducted in person and an understanding of individuals' thoughts and experiences were not lost in translation from another language. All nine participants interviewed for the study used Google and had a Gmail address. However, only seven actively used Gmail and only five of the participants used Google when logged into their Gmail account. Beyond the qualifying characteristics, demographic information was not asked of participants.

Interview Procedure

To ensure fluidity and opportunity for understanding users' language, meanings, and experiences, a semi-structured interview protocol was developed and used with an interview guide to establish rapport. Some questions on the guide were not applicable and therefore not asked during interviews while other questions not on the guide were asked impromptu during the interviews. (Interview questions can be found in Appendix B.) Interviews were conducted in participants' homes or in coffee shops, lasted approximately 20 minutes, and were audio recorded with participants' consent for transcription and analysis purposes.

Thematic Analysis

Following a verbatim transcription of each entire interview, participants were assigned pseudonyms to maintain their confidentiality and privacy. To sustain this confidentiality and privacy no pseudonyms were used when quoting participants' responses. Using previous research and examples by Boyatzis, 1998; Braun & Clarke, 2006; and Thomas & Harden, 2008; inductive or data-driven thematic analysis was used to analyze each interview transcription. This process was chosen because it focuses on patterns or themes within the data and would provide information on how the participants define privacy within each context. Each interview was read, edited to remove unrelated material and organized by corresponding context, e.g., information regarding Gmail was separated from information related to the privacy policy. Each context or set of data was then examined for patterns and similarities among all the participants' responses to establish inductive themes, or patterns found within the data, e.g., every participant explained privacy as maintaining control over personal information. Once these inductive

or data-driven themes were identified, codes were created to describe and differentiate the themes. Codes are the descriptors of each theme and can include name, characteristics, indicators or flags, qualifiers and exclusions, and examples. These codes were developed through and included users' words and phrases, e.g., the code of personal information consists of "name," "social security number," and "family," but excludes "public" and "for everybody to know." These codes allow for the theme to go from an abstract pattern to a conclusive finding of how the participants define privacy in each context. After developing each theme's codes, transcripts were reviewed again to ensure the theme(s) for each context were accurate. The use of the interview transcription data in this inductive thematic analysis process allowed for the participants' language, meanings, and experiences to become the codes and themes and thereby maintain participants' conceptions and perceptions of privacy for each context when defining privacy.

After identifying and understanding the inductive or data-driven themes in each context and discovering the participants' different privacy definitions, deductive thematic analysis was used to examine Google, Inc.'s March 1, 2012, privacy policy since none of the participants had read the new privacy policy and so they had no conceptions or perceptions of Google, Inc.'s updated privacy practices. Deductive or theory-driven thematic analysis was necessary to maintain participants' privacy conceptions and perceptions while further understanding how their privacy definitions and expectations align with Google, Inc.'s March 1, 2012 privacy policy. Deductive or theory-driven thematic analysis follows the same procedure as inductive or data-driven analysis except the data is not examined for themes in deductive, theory-driven, thematic analysis (Boyatzis, 1998; Braun & Clarke, 2006; and Thomas & Harden, 2008). Instead,

deductive thematic analysis uses a theory or theories to examine, code, and analyze the data (Boyatzis, 1998; Braun & Clarke, 2006; and Thomas & Harden, 2008), e.g., participants' defined privacy as maintaining control over personal information, so what does the privacy policy say about users' maintaining control over their personal information. While inductive or data-driven thematic analysis provided a rich description and understanding of the participants' perspectives, deductive or theory-driven thematic analysis provides an opportunity to examine in-depth users' privacy perspectives and the Google, Inc. March 1, 2012, privacy policy (Boyatzis, 1998; Braun & Clarke, 2006; and Thomas & Harden, 2008). The theories used for deductive analysis of the March 1, 2012, privacy policy were the participants' privacy definition themes that were discovered during the prior stage of inductive, data-driven, analysis. Since different privacy themes were discovered for each context, the March 1, 2012, privacy policy was analyzed multiple times according to each context's theme or theory. The use of participants' contextual privacy themes as theories was essential to maintain the users' understandings of privacy. This also allowed for Google, Inc.'s March 1, 2012, privacy policy to be analyzed according to participants' privacy definitions and expectations and ascertain how their privacy conceptions and perceptions align with the reality of how Google, Inc. states users' privacy is handled.

CHAPTER FOUR: FINDINGS

The goals of this study were to determine how some individuals conceptualize, perceive, and define their privacy, how their privacy definitions translated to Internet with Gmail and Google, and if and how their privacy assumptions and expectations align with Google, Inc.'s privacy practices. Participants' privacy definitions and conceptions in a general sense, with Gmail, with Google, and while Googling in Gmail are addressed first, followed by their perceptions of Google, Inc.'s March 1, 2012, privacy policy. Finally, while not discussed with participants during their interviews, the reality of Google, Inc.'s privacy practices per the March 1, 2012, privacy policy is examined.

Defining Privacy

Privacy in General

All of the participants described a similar theme of maintaining control over personal information as their definition of privacy. In this theme, "maintaining" describes the choice, decision, or right to decide; "control" means who knows, who has access to, and who is included in sharing; and "personal information" includes non-public details, facts, and events of one's life.

The participants expressed this sentiment of privacy through statements such as "privacy to me is being able to know the information that you don't want other people to know is safe … safe mean[ing] they can't become aware of the information," "private life

is stuff that I don't want to share with other people. It's private, it's personal … versus the public, the public me there are things that I'm okay with other people knowing about me doing," and "it's stuff that I don't want other people to see, that I wouldn't be comfortable with everybody having access to." This emphasis on not sharing, letting, or allowing others know something was described by other participants as "if something is intended for me, controlled by me, and a legitimate understanding that it's yours and you have control over it and someone violates it, that's privacy," "pretty much anything and everything I consider is my business and if you don't need to know, you're not going to find out," and

> Privacy is, is your right, your ability to maintain some sort of personal, I mean, it's everything from pictures that you share to information that you should so choose if you want to, you know, it's your name, your social security number, your family, your everything…. My right, my privacy being my right. Well yeah, it should be your right, if you don't want to share anything about yourself you shouldn't have to, I mean, it's you.

The examples of "stuff," "information," and "my business" participants provided consisted of knowledge about oneself they deemed personal and varied among them. A couple participants considered their driver's license number, address, anything that could affect another's opinion of that individual, and "anything where I am enclosed, I feel like in my own private space" to be examples of privacy. The examples shared among the majority of participants included financial information such as credit card numbers and bank statements, social security numbers, daily life activities, Internet and computer activities, emails, photographs, "any information," and "everything." As one participant expressed, "private information, it depends on the person that I would want, that's looking at my information. It could be anywhere from a picture to my social security

number." Another participant elaborated on privacy in different, specific situations and parameters:

> Privacy is that I, I choose what of my personal life is put out there, like on social networks, and that if I say to a person "I do not wish to discuss that issue" or "it's none of your business," that doesn't mean I'm, you know, ashamed or hiding anything, just that it's personal, private, again that word, that it's, it's mine to decide. If I'm in my home, I feel like I have a level of privacy and security that people just can't come prancing in and tell me what to do. I mean that's pretty much it. My social security number shouldn't be blasted out there for everybody in the world to know, my driver's license number isn't for everybody to know, you know, like, my bra size isn't for everybody to know, privacy.

Participants also included statements clarifying their definition from how others might define or explain privacy. While one participant's clarification was simply, "it depends on how you define privacy," another elaborated on how others might think about privacy and that privacy is ultimately determined by the person defining it:

> Privacy is just, it's everything, it's all encompassing. If you don't want to share what time you wake up in the morning, you shouldn't have to. You shouldn't have to say what color underwear you wear, um, you shouldn't have to say how you're feeling, you shouldn't have to, it's private. It can be, there are people that share everything and there are people that don't share anything and it's, I guess, privacy is all in the eye of the beholder. It's what, some people don't view talking about what medications they take as being private, some people would never disclose that they even take medication, so everything is personal, everything is [*sic*] personal.

Privacy with Gmail

Participants' definitions of privacy when using Gmail were similar to their definitions of privacy in general, in that only the account owner should have access to the account and any entity other than the account owner going into the account and viewing the account emails, information, or records is a violation of privacy. As one participant said, "privacy to me when I'm using Gmail is more about not letting other people have access to my Gmail, having access to my Gmail account."

This theme of no "unauthorized" access or no access to the account by anyone other than the account owner was expressed by almost all of the participants. Participants' examples of owner-only access included virus and hacker prevention; "my own personal Gmail account, that's it's just it, it's mine, and it's, that it not be monitored;" emails viewed only by the sender and recipient(s); and email drafts visible only to the account owner. As one participant explained, information in emails sent, received, and drafted are not for everyone to see:

> Only the person that I'm sending or receiving the information from can see it and I especially wouldn't want anybody to see information that I'm currently typing or haven't sent to anybody, so if it like auto saves it, I don't want anybody to be able to view that or watch me as I'm doing something.

The list of unauthorized entities participants did not want accessing their accounts included the government, Google, Inc., employers, friends, family, and hackers. One participant discussed the eternal nature of emails and information and the potential access by the government:

> The government has access to everything should they ever need it … there are things that I would never divulge during email because it's in writing forever…. what I say is there, forever, I may have deleted it and never be able to find it, but somebody somewhere has access to it.

Another participant explained the discovery of Google, Inc.'s practice of accessing emails for advertising purposes:

> Whenever I had an email that had, that was about a subject, it would always have that subject listed on the side with advertisements for it, or um, suggestions of other things to look at, other sites to look at, stuff like that…. So I feel like obviously they have something, some sort of program or something, that's looking into my emails or accessing my emails and then taking information from them, so in that sense I feel like obviously if they can access it, if they're looking at it, it's, the program or whatever is accessing my emails then it's, it's not private, something else, someone else is looking at it, that's what I think.

Despite this participant's awareness of Google, Inc.'s practices, Gmail use was immutable: "I keep using [Gmail], so obviously I didn't care too much about it."

Privacy with Google

In contrast to privacy with Gmail, thinking of and describing privacy when using Google separated participants between those who do not expect privacy and those who don't think about privacy while searching. Two thirds of participants did not consider their Google searches to be private and "had no expectation of privacy" while using Google. As one participant described, privacy doesn't exist on a public web site:

> Um, (long pause), I don't, I don't think I could [describe privacy when using Google]. I don't know how private Google searches are. I don't consider them to be private, I feel that if you look something up in Google then, I mean, I've never thought of searching, anything on any site for that matter, is private.

The six participants who did not consider using Google, or Googling, private expressed similar views from which four codes emerged: tracking, mining, profiling, and targeting. Based on participants' responses the codes can be defined as the recording of user information and searches (tracking), gathering recorded information and associating it with a user (mining), compiling user information to form generalizations about that individual (profiling), and showing specific advertisements that are likely to be of interest to that user (targeting or targeted advertising). One participant explained with conviction that Google is seeing users' information:

> I know that Google tracks, I know Google tracks the searches and I'm sure that there's somebody that sees that eventually, it's like when you can look up popular searches, so I figure if I'm searching for it, somebody has access to it.

Google's list of most popular searches, auto-complete searching (where the most popular search phrases are offered based on what the user is typing), and flagging or prevention

of "inappropriate" searches and sites by an external source were expressed by participants as sources of awareness to Google's lack of privacy and tracking. As one participant said, "as a matter of fact, I know that places, like [at school], if someone is searching for something inappropriate, I think they have red flags that trigger some sort of alarm somewhere." One of the participants with no expectation of privacy also emphasized the "economic value" in "the whole game" of tracking, mining, profiling, and targeting to "capitalize off" users:

> That's how they make their money, they're mining data, mining my personal, they're mining me, and they're trying to figure out, with precision, they probably know, they can go down to where I live, what I search for, preferences whenever I use it.

While no other participants referred directly to Google, Inc.'s profits from the sale of their data, most participants felt that the practices of tracking, mining, profiling and targeting were universally employed. The widespread public use of Google by individuals was frequently mentioned when describing whose and what information is tracked and mined. As one participant stated, "I would assume that's [*sic*] data [is] gathered from everybody, so it's not necessarily a private search engine." Another participant explained how searches are logged and accessed to determine what is being searched and by whom:

> They have like top searches so I realize that somehow they're keeping track of what people are searching. So it's not like, I go in there and search for something and no one else is going to see it and no one is keeping track of it. It's like, you know, this search is being logged somewhere and they're keeping tabs of what the most common searches are. So obviously somewhere else or something else is accessing my searches and saying this person is searching this.

Participants' awareness of recording and gathering information also led to comments on the absence of privacy with profiling and targeting. One participant explained the

annoyance and frustration of being automatically classified and feeling a loss of choice in what is received and viewed due to spam and sponsored websites[5]:

> When I type in something, how are they tracking this, how are they deciding, are they using this to build like an online profile of people, like, oh they look for this, so they're probably interested in this …. Just because I Google search [on a certain subject], I don't need to be thrown into and go to a certain website. I don't want to be thrown into everybody's spam, that they make [assumptions] and send me. If they start seeing a trend, that I'm a [person with certain interests], that I don't start getting everything. I want to be, I want to choose which sites I go to and look at.

While two thirds of the participants acknowledged and expected no privacy when using Google, the other third did not think about privacy or associate privacy with Google. "I guess I never really thought about it with search, actually," one participant explained. "I just never thought about it …. I've never noticed anything bad coming about from using Google, like with my information's been given out. I guess I never really thought about it." Another participant stated that privacy had not been considered when using Google because the searches conducted were to find information: "I guess I really don't think of privacy too much there …. mainly I'm using it to find information …. When it comes to [searching], I really don't, uh, consider privacy, you know, as an issue."

Despite the participants' perception of no privacy or lack of privacy conceptualizations when searching with Google, nearly all of the participants also expressed sentiments of "I'm not concerned" or "not too worried." This lack of concern by almost all of the participants stemmed from the widespread public use of Google and dissociation between their searches and personal information. As one participant

---

[5] The websites that have paid to be in a lightly shaded box at the top of the search results pages.

described, the absence of users' information with the list of most popular searches diminishes any concerns about privacy:

> I think because it's gathered from everyone it's not really a big concern. It's not like I'm going to start typing something in and it's going to be like so and so from Tennessee asked the very same question two days ago at 4pm. You know, it's not going to bring that up, it's going to bring up a popular search that somebody else has searched repeatedly or maybe even from that particular that it's linked up to, this is the most common search.

Other participants also mentioned their belief that searching for information did not provide Google with any personal information about them: "I'm looking for information, so I don't really know how much access they have to any personal information when I'm searching for [a specific topic] or something like that. There's not really much, you know, that I'm concerned about privacy there."

Privacy when Googling in Gmail

While not originally part of the research questions, participants' conceptions and perceptions of privacy with Google while logged into their Gmail was included after the first participant mentioned searching on a Google, Inc. phone. Since Google, Inc. stores users' searches in their Gmail account when they are logged in, this question was added to the interview script. Of the five participants who Google while logged into their Gmail accounts, four of them had "never really thought about [their privacy]." Participants' responses centered on the theme of not associating or correlating searches with email accounts: "No, I never really thought of it. I just realized, yeah, I didn't realize I'd be in my Gmail account, I'd just search, I use Google a lot." As one participant described, this unawareness of the collection and compilation of information into the user account comes from the different functions of and dissociation between the services: "as far as searching

when I'm logged into a Gmail account, I never think of it; whenever I Google search, I'm just searching." While three of these participants would prefer not to have their searches associated with their Gmail account, they recognized that the connections have already been made and expressed an "oh well" attitude: "Um, it's fine, I get a little annoyed with it, but I, you know, I'm not that concerned about it."

The only participant who does think about privacy tries to remember to log out of the account before searching, because "I don't want my searches being saved … I prefer anonymity." However this participant's prevention of searches with account information contrasted with another participant's appreciation of the saved search history within the account:

> I have noticed that when I am linked into a Gmail account and I'm Googling something that it will bring up my past searches and I'm completely fine with that because a lot of times I am looking for a previous page that I've been to and I just couldn't remember the URL and am like, "what was that page?" and go through and find it cuz it was logged in my history, which was fantastic.

The New, Unread Privacy Policy

While the use of Google does not require users to acknowledge acceptance of Google, Inc.'s privacy policy, Gmail users are required to check a box accepting the privacy policy but only during initial account setup. When Google, Inc. revised and implemented the March 1, 2012, privacy policy users were notified and their continued use of Gmail and Google was regarded as consent to the new privacy policy changes.

Out of the nine participants interviewed, not one had read the new Google, Inc. privacy policy that went into effect nine months earlier on March 1, 2012. Two of the participants did not know there was a new privacy policy, three said they "might have

heard" about it and four participants knew about it. When asked why they hadn't read the privacy policy, participants' responses could be categorized into six themes: unimportance of the privacy policy, trust in Google, Inc., assumptions associated with legal policies, use of the product anyway, uninformed on privacy policies, and access to personal information. While these six themes can be similar and overlap, what makes them distinctive in this study are the participants' lengthy and inclusive explanations. Every participant talked about almost every theme in their explanation as to why they hadn't read the new privacy policy.

Unimportant

"Um, because there's other more pertinent things in my life that I need to pay attention to than Google's privacy information," is one of the responses a participant provided explaining why Google, Inc.'s new privacy policy had not yet been read. Many of the participants expressed similar statements about reading the privacy policy as not important enough to warrant their attention, whether or not they were aware of the new privacy policy. One participant "didn't think that there was any reason to really look into it," while another just didn't feel like reading the policy. Some participants said they were too busy and "didn't have the time:"

> It was the last thing on my mind to read a privacy policy that was 2, 3 months before my [personal event]. So I just didn't really take the time and it hasn't, haven't had the time to read it.

Others are waiting for a news article about the policy before they decide whether to read it:

> So, I follow more through articles that I read in the media and then if something I find insightful and usually they're contradicting, someone is contradicting what is

> in the policy and there's some discussion or excuse, I'll follow that train or thought before I just read their policy.

Another participant commented on the unseen effects of privacy violations:

> I mean, you know, technology encroaches daily upon that very fine gray line between what's cool and what's not. But I think a lot of us don't really think about [privacy] too much cuz, I know I don't some days, because we're, we haven't seen the effects of it on our, on us.

Trust

"I'd already signed one previously, I'm not really plussed [nonplussed] at what the new one says. I have a certain amount of trust in the Google Company and brand name now." This participant's response succinctly defines the "trust" theme: participants do consider and are concerned about their privacy, just not with Google, Inc. Participants' expressed trust in Google, Inc. also meant they did not associate or consider the topic of privacy with the company. As several participants commented, "I'm not concerned about my privacy with Google, Inc." and,

> I just never thought about it …. [I'm] not really not concerned, I am concerned about privacy. I just, I never put two and two together. I guess, I never thought about there being an issue of privacy with Google.

Legal Policy Assumptions

Another theme among participants' responses focused on how they think about and what they associate with privacy policies: "It's like 30 freaking pages long and it's written by attorneys and unless you understand that [expletive], I always go down to the bottom, hit accept and continue." Long, boring, legal jargon, sleep-inducing, difficult to understand, unclear meanings, and time consuming were responses nearly all the

participants stated as reasons not to read the privacy policy. One participant expressed the frustrations in trying to read the legalities of privacy policies:

> If they're going to be posting their privacy policy, policies, they understand that not everyone can understand, you know, legal jargon and know that every word has a very specific purpose and it must be defined. I mean having "and" or putting in "or" or "but" into a sentence changes the whole meaning behind it and not a lot, not everybody knows that or that some terms need to be, are very sensitive, and need to be defined. As far as privacy, what do they mean is privacy? Do they include that is social security number or, you know, your home address? Somebody else might assume that's what it is, and if it's not clearly defined in there, and they can go and find certain definitions of what they mean by certain terms, then you can be assuming, and we all know what happens when you assume, and it's, it can be a huge issue for some people.

Another participant also discussed the issue of unclear meanings and undefined vocabulary and suggested that revised privacy policies should include a summary of changes and explanations of terminology. This "summary page" would alleviate the problems these participants associated with legal privacy policies:

> I don't have time to sit and read. I suppose it would be nice if they had a, I don't know if they do or not, but a summary page or like a bullet point of what the main changing points, because I don't have time to sit there and read their pages upon pages of information that says, in words that repeat itself a whole bunch of times so I'm not really sure what's going on, and second of all, say things that I don't really understand. So, and like, the vocabulary and their wording, I would just like some main bullet points then it would, if it referenced, if I didn't understand or wanted to know more about the bullet points, it'd reference a certain page saying "if you want to know more about this you can read this paragraph and page."

Use Anyway

"I don't read [the privacy policy] because I feel like I'm going to use this service whether they have one or not, unfortunately…" is a defining characteristic of this theme. Multiple participants expressed the concept of "just click accept and continue" because they were going to use the product despite what the company's privacy policy stated. One participant perceived a disregard of the privacy policy by individuals because of a desire

to use the service or product no matter what. As the participant described, these benefits outweigh the expenses:

> But, you know, how many people actually read that whole [policy] before they actually hit that install button? You have all that, they have all that stuff to read, how many people actually read all that stuff? … You're spending a couple hundred dollars on a program from [company], you know, this is the new [operating system], whatever, whatever the new thing is, you know, how many people are going to read all that privacy policy [expletive] and not just click "Install" or "Accept"? … If it [is] something they feel they need or they have to use to, you know, they're going to; they're not concerned about that [privacy policy].

Uninformed

Participants' lack of knowledge about different privacy policies embodied this theme of being uninformed. One participant commented on not knowing if and what differences existed between privacy policies despite never having read one:

> I think if I was more aware of the different policies, if there are even different policies on privacy, I might be more willing to go for the one that had a more stricter privacy policy …. But yeah, I feel like, if I was aware of it, like if I was, I mean I'm aware there's policies, I just, I always feel like they're always the same, even though I've never ever read one, it's just this imaginary thing I made up in my head that they're all the same.

This feeling of not knowing about privacy and privacy policies was common among some of the participants. One of the participants commented that while concerned about privacy, had never thought to try and find the privacy policy:

> I didn't even think about checking out, I guess I don't think about, I don't even … I didn't even realize that you could look stuff up like that and check it out and see what their thoughts and views are.

Access to Personal Information

The theme of access to personal information was split between availability and withholding of individuals' personal information and user data. Participants from both perspectives of access to personal information noted this theme as a reason in explaining why they hadn't read the privacy policy. Some participants felt that they already allowed online companies to access their personal information through use of the company's products and services, so they didn't need to read the privacy policy. Other participants felt they were cautious and did not divulge any personal information when using companies' products and services, so they didn't need to read the privacy policy since it wouldn't apply to them.

One of the participants whose personal information is available described accepting or agreeing to a company's privacy policy as "signing your life away:"

> When you agree to a privacy policy act of any kind, policies and procedures, you have inadvertently given access of your information to another corporation …. So when you do that privacy policy act and sign your life away you are giving a little piece of you to the company that is accepting it.

This relinquishment of personal information to companies does not stop with the company, but extends to the entire "online world and online community." Since activity on the Internet is "part of who I am" and is "in theory, viewable by others," authorized companies can rightfully view individuals' information, leading some users to conclude that it does not matter what the privacy policy says or if they read it.

In contrast, another participant who does not provide personal information focused on the accessibility of personal information through viruses, spying, and hacking:

> I'm pretty careful about what I share with people, as far as personal information… I try and generalize a lot of stuff so I don't really feel like I'm putting too much

> personal information out there. So I just don't really think about oversharing or giving out too much personal information …. I've always heard growing up, be careful what you put on the Internet because you never know who or what might be looking at it.

The awareness of peering eyes and access to personal information was mentioned by several other participants as well: "I realize that pretty much anybody can see anything, so I try to be careful about what I do, how much information I give out." This wariness of privacy led some participants to believe the privacy policy is not relevant to them since they aren't "providing" any private information and therefore they don't need to read it.

Privacy according to Google, Inc.'s March 1, 2012 Privacy Policy

Since none of the participants read the March 1, 2012, privacy policy, they did not have conceptions and perceptions of privacy based on the terms of the privacy policy. Instead, participants' privacy definitions and expectations were used to examine how the company defines and handles users' privacy according to the privacy policy.

Users' Information

> We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful or the people who matter most to you online. (Google, Inc., 2012, "Privacy Policy")

Google, Inc. states they collect information from its users, however the type of information depends upon how it is collected. Google, Inc. distinguishes between information they ask for and users' provide and information collected from using their services:

> We collect information in two ways:
>
> - **Information you give us.** For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card. If you want to take

full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.

- **Information we get from your use of our services.** We may collect information about the services that you use and how you use them, like when you visit a website that uses our advertising services or you view and interact with our ads and content. This information includes:
    - **Device information**
    - **Log information**
    - **Location information**
    - **Unique application numbers**
    - **Local storage**
    - **Cookies and anonymous identifiers** (Google, Inc., 2012, "Privacy Policy")

Google, Inc. explains that "we use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services" (Google, Inc., 2012, "Privacy Policy"). Additionally, Google, Inc. may associate the information collected about a user with the users' account and personal information. Google, Inc. combines this collected user information into a single user profile:

> We may use the name you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account so that you are represented consistently across all our services. If other users already have your email, or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo. … We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. (Google, Inc., 2012, "Privacy Policy")

Despite how many participants would like for their Gmail account information and emails to be private to only them, Google, Inc. collects their information. Google, Inc. collects both provided and gathered information from every user whether the participating Google users know there is no privacy or don't think about privacy and

aren't worried about their personal information, be it non-personally identifying, personal, or sensitive.

Access to Users' Information

No matter what product or service an individual uses, Google, Inc. accesses users' information and accounts to collect information for tracking, mining, profiling, and targeted advertising. In addition, Google, Inc. utilizes users' information to improve their services:

> We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads. (Google, Inc., 2012, "Privacy Policy")

In addition to Google, Inc. having access to users' information, associated third parties are given users' information for external processing and other reasons. Google, Inc.'s Privacy Policy discusses the continued sharing of users' non-identifiable information:

> We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures …. We may share aggregated, non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services. (Google, Inc., 2012, "Privacy Policy")

If an individual is accessing an account to use Gmail or Google through an employer via Google Apps, that user's account information and activity is available to the company or organization as well as Google, Inc. As Google, Inc. states:

> If your Google Account is managed for you by a domain administrator (for example, for Google Apps users) then your domain administrator and resellers who provide user support to your organization will have access to your Google Account information (including your email and other data). Your domain administrator may be able to:

- View statistics regarding your account, like statistics regarding applications you install.
- Change your account password.
- Suspend or terminate your account access.
- Access or retain information stored as part of your account.
- Receive your account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.
- Restrict your ability to delete or edit information or privacy settings. (Google, Inc., 2012, "Privacy Policy")

Government access to participants' emails, searches, accounts, account information, and additional information is also possible as Google, Inc. stores identifying data and states that they will share information for legal reasons. Google, Inc. explains:

> We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
>
> - Meet any applicable law, regulation, legal process or enforceable governmental request.
> - Enforce applicable Terms of Service, including investigation of potential violations.
> - Detect, prevent, or otherwise address fraud, security or technical issues.
> - Protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law. (Google, Inc., 2012, "Privacy Policy")

While this study's Gmail participants might not want anyone other than themselves to have access to or know their information, it is available to Google, Inc., employers, the Government, and affiliated third-parties. Additionally, if the Google participants in this study knew of this list of entities that have access to their searches and associated information, they might be more concerned about their privacy.

CHAPTER FIVE: DISCUSSION

The findings of this study answered its research question on how some individuals define and think about privacy in general, with Gmail, with Google, when Googling in Gmail, and with Google, Inc. This study also examined how the users' privacy expectations and assumptions translate to Google, Inc.'s privacy practices per the March 1, 2012, privacy policy. As the participants in this study demonstrated, privacy means different things to different people. And yet their definitions of privacy for each context were analogous to each other, though not necessarily with Google, Inc.'s privacy policy.

Privacy Depends

Although all of the participants defined privacy, in general, as maintaining control over personal information, their definitions and descriptions of privacy varied amongst them. For example, participants' differences in defining privacy led to various descriptions of what privacy entails and when it exists. This broad range in responses as to what constitutes personal information can be attributed to the contextual nature and individualistic perspective of the word "privacy."

The context of "in general" is broad and vague, as demonstrated by the participants' responses, and narrowing the parameters alters one's expectations and thus, definitions of privacy. Some of the participants demonstrated this by elaborating on their definitions of privacy in specific contexts such as social networks, the home, others' homes, and personal property. These contexts also demonstrate how "privacy" can

sometimes be difficult to define as everyone has a different meaning, expectation, and understanding of what privacy is to them, especially in different situations. However, the participants' collective broad definition and theme of privacy as maintaining control over personal information allows for a general understanding of privacy, in any context, while incorporating each individual's own specific meanings, expectations, and understandings. This privacy theme also extends to the participants' definitions of privacy with Gmail, but the change in context from Gmail to Google and Googling in Gmail, intriguingly led to different conceptions and perceptions of privacy.

Gmail

Participants' conceptions of privacy with Gmail were similar to their thoughts of privacy in general, except they were, expectedly, centered on access to emails, records, and account information. In addition, the description of "people," generally speaking, changed from anyone to more specifically the Government, Google Inc., employers, hackers, family, and friends. All of the participants described privacy with Gmail as user-only access to their emails and information. While this privacy theme aligns with participants' theme of privacy in general, it is, contrary to the Gmail privacy practices.

Participants' conceptions and expectations of Gmail privacy as user-only access were intriguing given the email's structure. Even without knowing or examining the privacy policy, Gmail's spam filtering and advertising suggests that emails and the information within are being read, scanned, or viewed by someone or something. The inclusion of the Government on the participants' "no access" list to their emails was anticipated since most Americans don't like the idea that "Big Brother" is watching. However, Google, Inc. can provide Gmail users' information to the Government if it is

requested. Such requests for Gmail users' information rose 133% from 2011 to 2012 in the U.S.: 12,271 requests for user data (e.g., emails and searches), and 23,300 requests for users or accounts (i.e., personally identifying information), were made in 2011 compared to 16,407 and 31,072, respectively, in 2012 (Google, Inc., n.d., "Transparency Report;" Google, Inc., 2012, "Privacy Policy"). In addition, Gmail users' emails and information are shared with company or organization administrators running Gmail accounts, and information that is not personally identifiable can be shared with partner companies, organizations, and individuals outside of Google (Google, Inc., 2012, "Privacy Policy"). While Google, Inc. does take precautions to protect its users' information, such as encryptions and restricted access, there is no guarantee hackers won't access individuals' information (Google, Inc., 2012, "Privacy Policy").

While the participants' privacy conceptions and expectations with Gmail are justifiable, unfortunately they do not coincide with Google, Inc.'s privacy practices. Google, Inc. accesses Gmail users' emails and provides users' information to employers, the Government, and itself. While the company does address information security in the privacy policy, that does not mean users' information is guaranteed to be safe as secure Internet networks and databases can be hacked. In addition, emails can be forwarded to anyone, including family and friends, without the users' knowledge. Perhaps more troublesome is that as American society becomes more dependent and focused on technological advancements, the erosion of email privacy will continue if companies and employers continue to collect information, Governmental requests for users' account and data information increases, and hackers, family, and friends become more technologically savvy.

Google

Contrary to participants' views on privacy with Gmail, their conceptions and perceptions of privacy with Google were nonexistent or unconsidered, but nevertheless unconcerned. The majority of participants discussed the absence of privacy with Google since the search engine is publicly available, monitors and records searches as demonstrated by the list of most popular searches, automatically completes search phrases, and flags or restricts access to certain websites. Additionally, a few participants talked about advertisements related to previous and current searches and the awareness that Google, Inc. is collecting users' search information to learn about them and create a more detailed user profile. The few participants who had not considered privacy when using Google thought they were not affected by the information collection or believed that the collected information was not personal. For these individuals the act of searching for information and the absence of a visible association between the search and their information allowed them to be oblivious to their privacy. Despite the participants different privacy conceptions with Google, the vast majority of them expressed an unconcerned attitude toward their privacy with Google. This nearly unanimous lack of worry from participants about their privacy emanated from the public use of and impersonal aspect of searching and therefore, dissociation between searches and personal information.

While the participants' theme of the absence of privacy with Google contradicts their general definition of privacy, it coincides with the Google, Inc. privacy practices. Google, Inc. does collect information about its users, including what they are searching for, and utilizes that user information to tailor individual screen content which is why

some of the participants who perceived an absence of privacy also noticed relevant advertisements (Google, Inc., 2012, "Privacy policy"). The few participants who hadn't considered their privacy with Google were in keeping with their general privacy definition as they believed they were maintaining control of their personal information. However, Google, Inc. has been cognizant of their personal information the entire time they have been using Google. Unfortunately for these participants, whether they considered the personal aspect of searches or saw the effects of their collected information, Google, Inc. is constantly collecting data on its users and how they use Google, Inc. services to learn more about them and assist in the delivery of personalized content (Google, Inc., 2012, "Privacy policy").

Whether the participants were in agreement or disagreement with the privacy policy, the most intriguing theme among the majority of participants' conceptions and perceptions of privacy with Google was their unconcerned attitude. Despite two thirds of participants expressing an awareness of tracking, mining, profiling, and targeting, their worry-free sentiment stems from their perceptions that searches are public and impersonal. Although Google, Inc. collects data from all its users around the globe, that doesn't mean the information cannot be and is not associated with individual users through device information, IP addresses, and cookies (Google, Inc., 2012, "Privacy policy"). In addition, while the information collected about the participants may not be the specific examples of personal information they defined in their general privacy definition, it still communicates something about them to Google, Inc. (Google, Inc., 2012, "Privacy policy"). Lastly, as with Gmail, users' information collected through

Google is available and can be disseminated to the government and employers (Google, Inc., 2012, "Privacy policy").

Googling in Gmail

Similar to Google, the majority of participants' conceptions and perceptions of privacy when using Google in Gmail were unconsidered and unconcerned. Although two of the participants were aware of the absence of privacy while Googling in their account, they diverged on their privacy conceptions. The participants who had not thought about and were not worried about their privacy did not recognize the direct association and compilation of Google search information with their Gmail accounts. However, those participants' acknowledgement of this connection between Google and Gmail included a resignation of their privacy loss. Contrastingly, two of the participants comprehended the absence of their privacy when Googling in Gmail, but were divided on liking or disliking the saved search history within their accounts. Their divergence suggests a difference in their value of privacy: one prefers personalization over privacy while the other prefers privacy over personalization. Despite the differences among these participants' privacy conceptions and perceptions with Google in Gmail, Google, Inc. combines users' Google searches with their account information when they are logged in (Google, Inc., 2012, "Privacy policy").

Privacy Paradoxes

The findings of these contextual privacy definitions highlight contradictions in how the participants' conceptualize and perceive privacy: While participants expressed that they care about their privacy, they also stated they aren't worried enough about it to

read the privacy policy. Thus their expectations of privacy with Gmail contradict their expected absence of privacy with Google and their rationale for not reading the new privacy policy are also reasons to read the new privacy policy.

Care vs. Concern

The participants in this study demonstrated that they care about their privacy. While their overarching theme of privacy in general was that a definition of privacy depends on the expectation of privacy, participants, nonetheless, expect the choice and right to determine who is informed or knowledgeable of their life. Although privacy expectations can depend on the individual and context, as seen with Gmail and Google, participants expressed an overall desire for privacy. However, participants' preference for privacy is contradictory to their behavior as not one participant read Google, Inc.'s new privacy policy within nine months of its implementation.

Google, Inc.'s March 1, 2012, privacy policy was a significant event for the company; its users; the technology industry; national and international governments; and the academic, privacy, legal, technological, and legislative fields; among others. So the fact that all nine participants said they had not read the privacy policy that started a new round of privacy controversy with Google, Inc. was a bit surprising, especially given their expressed desire for privacy. Although Google, Inc.'s efforts to inform its users of the changing privacy policy were initiated only six weeks prior to its effective date, multiple participants stated they were personally notified of the changing privacy policy. In addition, Google, Inc. posted notifications on both the Gmail and Google homepages and the media covered this event from its announcement through its implementation. So if

participants truly care about their privacy like they said, why wouldn't they be worried enough about the changing privacy policy to read it?

Today's society is becoming more and more technologically dependent and individuals are using the Internet more and more for everyday activities of communicating, researching, social connections, entertainment, etc. While some of the individuals online may care about and want to protect their privacy, the amount of information associated with electronic privacy can be overwhelming. To attempt to maintain privacy online an individual has to know what privacy is afforded with the technology according to the privacy policy, and what privacy is desired. Given all the information individuals must consider and know to be aware of their online privacy, it is not surprising the participants cared but aren't concerned about their privacy.

To consistently be aware of and worry about one's privacy is exhausting, easily results in information overload or "information glut," (Postman, 1992, p. 70) and is also futile. Technologies are continuously being developed and improved which means their privacy policies are also likely to change. To be aware of and up-to-date on this information requires consistent dedication. And even the most dedicated privacy advocates face the frustration of the privacy policy legalities. Privacy policies are legal agreements on users' and company rights that every individual must consent to, implied or direct, before using the technology. To make matters worse, these policies do not favor individuals' privacy but rather company profits through the erosion of users' privacy. Google, Inc.'s CEO Larry Page exemplified this in his statement regarding the privacy policy change. Unfortunately for users there are limited options: concede and use the technology, find a similar technology with a privacy policy they are willing to agree to,

or don't use technology. While not using technology might be appealing, it is nearly impossible in today's technological society. Finding a privacy policy that favors the user is also extremely difficult as it is time consuming and rare, if not nonexistent and can lead to an information glut which can overwhelm and frustrate users. Overwhelmed and frustrated users are then likely to become part of the group that gives up and just accepts the technology and its privacy policy.

While this "inevitable use" mindset circumvents the overwhelming information glut, it also creates an attitude of privacy resignation. If individuals feel there is nothing they can do to avoid technology use and information glut, they may not give adequate consideration to what constitutes privacy and privacy violations, so why should they worry about their privacy? It may be easier for individuals to recognize that they want privacy but don't have it online and succumb to the "inevitable use" mindset, but that won't help them get the privacy they want. Individuals can make their voices heard by not using certain technologies and online companies or starting a petition against certain company's or technology's privacy policies because companies notice when a mass of users' are speaking with one voice. Additionally, individuals can make their demands for online privacy through privacy advocacy groups, rights groups, legislators, and policy makers so these parties can then incorporate the users' voices in the discussions of online policy.

It is in the current and future privacy concerns that resolutions can be found. Since individuals perceive emails to be private, discussions of Internet privacy should consider requiring separate and more stringent or more protective privacy policies for users' email. Instead of email falling under the general privacy policy umbrella, Google,

Inc. could have a specific product privacy practice for Gmail with greater privacy protections and rights. While stricter privacy regulations for email may not stop some external parties' access to users' email, they could provide users' with more rights to their privacy and greater reparations for privacy violations. Therefore it is through the users' voices and privacy concerns that Internet privacy discussions can include the different facets of users' online privacy, e.g., privacy with email is not the same as privacy with search, and future privacy policies can better reflect users' different privacy conceptions and perceptions for various Internet activities.

Gmail vs. Google

By not reading the privacy policy, participants' privacy conceptions and perceptions with Gmail and Google were limited to their expectations of privacy instead of their knowledge about Google, Inc.'s privacy practices. Participants' privacy conceptions with Gmail were unanimous on only users having access to email accounts. Contrastingly, participants' privacy conceptions and perceptions with Google were that privacy is nonexistent or unconsidered, and not concerning. These opposing conceptions and perceptions result in a contradictory belief about privacy with Google, Inc.: users expect privacy with emails but not when searching.

Unfortunately, the participants failed to realize Google, Inc.'s privacy policy and practices are the same for both Gmail and Google which means Gmail affords the same amount of privacy as Google. While Gmail does not have a list of "most popular" emails as Google does with searches, Gmail does have spam filtering and advertising which should suggest to users that their emails and information are being accessed by Google, Inc. Similar to searches, emails and the information within them are accessed and utilized

by Google, Inc. to profile individuals and target advertise. Although the participants cared about and expected their privacy with Gmail, most participants were unconcerned about their privacy with Google. However, participants may be more mindful of their privacy if they knew the entities that are able to gain access to their search and email information and user account data.

Despite Google, Inc.'s same privacy policy for both Gmail and Google, the participants' privacy conceptions and perceptions for these products suggest a translation of the privacy expectations and regulations from the offline to the online world. Gmail provides the service of electronic mail accounts where only the individual(s) with the account password has access to account information, emails received, and the capability to send or draft emails to others. The use of the account password to access electronic mail infers a privacy of the account similar to the privacy one is afforded with mail in a mailbox. While the United States Postal Service (USPS) technically owns the mailboxes individuals receive mail in, the mail belongs to the recipient and tampering with mail is a federal crime since the USPS is a federal agency (Branscomb, 1994). This federal regulation allows individuals to feel as though their mail is protected and private just as passwords allow email account owners to feel as though their emails are protected and private.

In contrast, Internet searches provide individuals the opportunity to access information in the public domain. For individuals to go online all they need is access to a computer with Internet connection capabilities. The Internet is a public domain that does not require a username or password for entry and can be searched on any topic. The Internet and online searching have condensed the process of looking for information in an

encyclopedia, phone book, library, etc. while extending the availability of information to everyone around the world. Individuals might not see Google's list of most popular searches as a privacy concern because it is similar to lists of "best-selling books," "top box office movies," greatest ticket sales or attendance for concerts or events, and the most watched sporting events or television shows. Most popular lists do not specifically state the individuals that participated and contributed to the ranking, just the statistics for each occurrence based on the number of individuals who took part in them.

These contradictory conceptions and perceptions of privacy with email and search reflect individuals' translation of their societal values, language, and knowledge from the physical world to the Internet. However, Google, Inc.'s privacy policy does not reflect these opposing definitions and expectations of privacy between email and search. The inclusion of this contradiction in privacy discussions would strengthen privacy policy reformative arguments and, hopefully, lead to separate privacy policies for Internet activities that are responsive to users' attitudes and expectations.

This contradiction of individuals' definitions and expectations of privacy also enlightens scholarly research as individuals' privacy conceptions and perceptions are individualistic and contextual. Although a theme or pattern could be found among participants' definitions within contexts, there were sometimes multiple themes within one context. This suggests that while individuals' definitions are similar and the individuals could be "classified," they need to be classified according to their perspectives, not those of theorists. In addition, while the participants' privacy definitions or expectations were similar and could be grouped, their specific privacy examples, such

as driver license number or personal space, differentiated them from one another. No two individuals thought and talked the exact same way about privacy.

The context of privacy is also important as participants' definitions and expectations of privacy depended upon the situation. These contextual definitions of privacy suggest that while individuals can define and exemplify privacy, those definitions and examples are unique to that context and cannot translate to a different one. While one privacy context cannot be applied to a different context, it can be transformed such as from the offline to the online world. Since privacy is contextual, the translation of the physical world to the Internet means the privacy expectations remain consistent but are adapted for the changes. For example, privacy at a public event or venue is the same as privacy when searching on the Internet: others know your interest, but they do not know your personal information. Since each person thinks about privacy slightly differently from others and this also depends on the context, individuals do not have one privacy definition and expectation, but multiple privacy conceptions and perceptions that will contradict. These contradictions among individuals' privacy definitions and expectations explain how privacy beliefs and behaviors can become paradoxical, e.g., information collection is okay from a "public" website but not from a "private" website even though both products have the exact same privacy policy.

Excuses vs. Reasons

Participants' provided six explanations for why they didn't read the privacy policy: lack of importance, trust in the Google Company, legal policy assumptions, use of the product or service anyway, lack of knowledge about privacy policies, and access to

users' personal information. While these reasons for not reading the privacy policy are valid, they are also all reasons to read a privacy policy.

Life can be busy at times, but individuals make time for the important things in their life. Despite an expressed care about privacy, Google, Inc.'s March 1, 2012, privacy policy was not important enough to care about and read for some of the participants. Additionally, Google, Inc. has evolved into a name and company that is known globally. It is known for the search algorithm which redefined searching the Internet, refusing to fulfill Government account and data information requests that are too broad or unreasonable, and the company motto "don't be evil." Google, Inc. has established itself as a pioneer in the technology industry developing products that have helped lead the way for technological innovations and improvements while becoming a serious competitor to existing online companies. While there are probably many more accolades to Google, Inc.'s name, the one most important to this study's participants was trust. Multiple participants stated that they trust Google, Inc. so there was no need to read the privacy policy. However, Google, Inc. also has a history of violating users' privacy as exemplified by the Buzz and Safari incidents. Given the multiple incidents of Google, Inc.'s user privacy violations, one would expect that privacy with the company may be a recurring issue and a changed privacy policy would be worth reading to know what users' privacy with Google, Inc. entails.

However, this study's participants are not the only individuals who dislike privacy policies that are long, boring, exhausting, time-consuming, difficult to understand, and have unexplained terms and unclear meanings. Users, policymakers, and advocacy groups all agree that privacy policies should be easier to read and understand, and

Google, Inc.'s March 12, 2012, privacy policy is, in fact, easier to read and understand. It uses plain language and all the technological terminology is defined, although not every privacy practice is spelled out in detail. The irony of this is that this study's participants did not read the new privacy policy because they wrongfully assumed it would be like just other legal privacy policies or that they were going to use Gmail and/or Google anyway. Yet this excuse of using the service no matter what is a contradiction in itself. If an individual is going to use a service, shouldn't that person want to know what it entails? Or, if an individual is going to agree to a contract, shouldn't that person want to know the terms of that agreement? By just clicking "Accept" users are not just acquiring use of the service or product, they are assenting to the terms and conditions of a legal agreement about their privacy with the product or service. This disregard for privacy policies is also why some of the participants felt uninformed on privacy policies. While it can be difficult to know about and understand the differences between privacy policies, it is impossible to learn the specifics and variations without reading them.

Finally, access to one's personal information divided participants between permission already granted and not providing anything personal. Some participants felt since they had already agreed to a prior version of the privacy policy Google, Inc. was allowed to access their personal information so there wasn't any reason to read the new privacy policy. Others felt that because they did not provide any information that could be deemed personal, so the privacy policy didn't matter and they didn't read it. However, both parties of this argument failed to acknowledge that a new privacy policy means changes have been made which can include greater access and use and a broader definition of personal information. By not reading the privacy policy, both groups are

unaware of what personal information entails and to what extent Google, Inc. has access to and use of it.

A Possible Explanation

These contradictions demonstrate the complexities of individuals' privacy conceptions and perceptions, and the difficulty of changing privacy contexts but not definitions and expectations. While participants' general privacy conception of maintaining control over their personal information can be applied to the context of the Internet, it must be altered as individuals' give up their control over who knows, has access to, and is included in the sharing of their information to online companies. Although privacy contexts can be translated from the offline to the online, the structures of the physical world and Internet are vastly different and therefore change the knowledge about privacy from a historically legal perspective to a technological aspect.

The notion of privacy as a right in America is nearly 700 years old and the protections of an implied right to privacy are almost 200 years old. Because the American legal system is reactive and interprets laws when they are challenged, this has allowed greater freedoms and limited the determination of legal boundaries on what is acceptable and punishable, especially with individuals' privacy. Over time the changes in society and privacy were gradual enough for the legal system to stay present in the issues of the day. However, the rise in digital technologies and proliferate use of them over the last few decades has left the legal system behind and absent in the privacy issues individuals are facing. Instead of worrying about whether someone is publishing private information about them, individuals now face the concerns of unlimited collection and compilation of private information by online companies. Additionally, the ever-changing advancements

in technology and unpredictable future of technological privacy invasions can make legal actions feel ineffectual or inconsequential, but now is the time when they are needed most. Individuals have different conceptions and perceptions of privacy in different online contexts and these need to be included in the privacy discussions. If legislators, policy makers, and online companies would acknowledge this in their conversations about online privacy then Internet companies, like Google, Inc., could change their privacy policies to incorporate users' different definitions and expectations of privacy with email and search. These changes could bring the legal system and individuals back into the online privacy discussion while considering the technological privacy issues.

Americans have rights because of the liberal democracy, the democratic freedoms, initiated when individuals' sought knowledge for their betterment during the Enlightenment. When the founding fathers established the United States they wanted to ensure that the democratic freedoms learned and fought for over the course of history would stand the test of time. However,they never could have anticipated today's technologies and the resulting erosion of some of those liberal democratic principles. While individuals' were once able to have their voices heard in the lawmaking process, they are now too often drowned out by the companies and businesses behind the technologies and privacy policies. Instead of a country's government and systems "of the people, by the people, for the people" (Lincoln, 1863, "Gettysburg Address") the people are not being heard and are losing the rights their forefathers fought and worked so hard to establish for them. However, if individuals' are included in the online privacy discussions or if legislators, policy makers, privacy advocacy groups, and rights groups include users' voices in the privacy discussions with online companies, then today's and

future technologies are more likely to coalesce individuals' privacy and technology for future online privacy harmonization.

Contributions

This study supports and verifies previous research findings and answered questions not asked in previous studies of online privacy: how some individuals define privacy for themselves in the contexts of in general, Gmail, Google, and Google, Inc., and how individuals' expectations of privacy translate to the reality of how Google, Inc. manages users' privacy per the March 1, 2012, privacy policy.

This study encompassed previous privacy research and expanded previous privacy theories and applications by addressing and examining how users think about and perceive their privacy in their own words. Participants' privacy definition of maintaining control over personal information aligns with Westin's (1967) definition of sharing information, Tavani's (2007) theory of restricted access/limited control, Moore's (2008) control and access perspective, and Ramsay's (2010) first sense of privacy as control over information. Participants' emphasis on user only access to their Gmail accounts bolsters Kachhi and Link's (2009) and Turow and Hennessey's (2007) paradox of concern over privacy and personal information yet willingness to provide it, and Dinev and Hart's (2004) finding of privacy concerns related to information access and abuse. Participants' expectation of no privacy or inconsideration of privacy when searching with Google does not support nor contradict any reviewed previous research. However, this awareness and acknowledgement of nonexistent privacy or lack of privacy awareness highlights an unexamined issue that needs to be explored in future research.

The participants' reasons for not reading Google, Inc.'s March 1, 2012 privacy policy support Joinson et al.'s (2010) research findings that trust is the strongest predictor of self-disclosure and behavior, but contradict their thought that trust is established based on situational cues as opposed to preexisting attitudes. This finding also supports Park's (2011) findings that users understand information collection and use but not an organization's data practices and terminology, and corroborates with Viseu et al.'s (2004) participant responses of not reading the privacy policy, uninformed on protecting information, knowing and trusting the company, enjoying the personalization, and nothing to worry about. Additionally, participants' perceptions of the privacy policy aligned with Best's (2010) finding that participants are not worried about the lack of privacy, but conflict with the finding that participants' evasion of information practices and their reasons for consent to surveillance.

However, the use of participants' thoughts, meanings, and language on privacy also allowed for their perspectives and opinions to be learned since users' points of view have been unheard and are excluded from the privacy definition discussions and research going on today. By asking the individuals to define privacy in their own words unknown privacy conceptions and perceptions were discovered: the participants have different definitions and expectations of privacy in different contexts. While the participants' definitions for each online activity were autonomous in that they did not include the exact same examples and thoughts, the definitions did embody the same perspective: emails are private, searches are not private. These findings on participants' privacy conceptions and perceptions uncovered contradictions in individuals' beliefs and behaviors and their

rationale for these oppositions while providing new insights into how individuals define and expect privacy.

Scholars of privacy and communication need to take these individuals' distinct privacy definitions and expectations into account when studying privacy because individuals have discrete conceptions of privacy for different contexts. Individuals' understanding and anticipation of privacy depends on the situation, e.g., emails are private while Internet searches are not. Future researchers not only need to ask individuals about their privacy conceptions and perceptions for each context, but they also need to account for individuals' unique definitions within each circumstance. Only through making distinctions among individuals' privacy expectations in each privacy situation can scholars fully understand and incorporate individuals' privacy conceptions and perceptions into discussions about each privacy context.

In addition, future researchers can benefit from the theme within all of the participants' privacy definitions, the notion of a right to privacy. The translation of the participants' expected privacy right to the context of the Internet showed how their privacy beliefs and behaviors conflict and these contentions arise from the loss of privacy to online privacy policies. These discoveries help future research because they provide a better understanding of individuals' privacy and therefore pose new related questions, such as in what other online contexts do individuals' privacy beliefs contradict privacy behaviors and practices and how do individuals rationalize those polarities?

The findings of this research study can also contribute to privacy considerations, discussions, and decisions on the individual, local, national and global levels that are going on today. Having more information on how individuals' perceive and

conceptualize privacy, in general and with Gmail, Google, and Google, Inc. after the release of the company's changed privacy policy, allowed for a more thorough understanding of participants' privacy with email and search: users' define and expect privacy differently for email and search. These privacy expectation distinctions among Internet activities exemplify users' understandings of privacy in different online situations. It is important that individuals' privacy definitions for each online context be included in the Internet privacy discussions going on today to generate more complete conversations between Internet users; online companies; privacy and Internet advocacy groups; and national and international policy makers, and therefore improve the chance of privacy policy changes that reflect users' contextual privacy conceptions and perceptions.

This study's participants' privacy paradoxes demonstrate individuals opposing perspectives and online privacy erosion that can assist legal scholars in future studies and actions of privacy policies. The goal of a law is to set boundaries and as there are a few limited and outdated laws regarding privacy online, there are little protections for users' online privacy. Instead, users' are subject to the individual privacy policy of each technology that was written by the company owning the technology. Each privacy policy defines users' privacy for each context, creating multiple definitions of privacy in multiple contexts, all of which are legal. The superfluity of privacy policies illustrates how users' voices and subsequent legal reparations have been diminished and need to be reestablished.

The acknowledgement of participants' thoughts, meanings, and language when discussing their privacy conceptions and perceptions in this study gave individuals an

opportunity to be heard, understood, and included in conversations about online privacy. Currently, Google, Inc.'s March 1, 2012, privacy policy is being discussed by the U.S. government, EU governments, privacy advocacy groups, rights groups, and online companies. Unfortunately, Internet users, the group affected most in this issue, are not included in these discussions. This study showed that participants' expectations of privacy are not reflected in Google, Inc.'s privacy policy and that the exclusion of their voices from the discussion suggests that companies' use of individuals' information is valued over users' privacy. This exclusion limits the information and knowledge about users' perspectives that could enrich and enhance the conversation and promote change.

Future Research

This study accomplished its goals of understanding individuals' conceptions and perceptions of privacy in general and in the contexts of Gmail, Google, and Google, Inc, and how individuals' privacy perceptions translate to Google, Inc.'s March 1, 2012, privacy policy. However this study also poses new questions for future research and studies.

Although Google, Inc. does not provide demographic information on its users, the company provides products and services to users around the world. Given the recent legal actions by data protection authorities in six EU countries, a study conducted in Europe would provide a different perspective on how non-U.S. residents who have online data protection rights perceive privacy generally speaking and with Google, Inc.

Additionally, the interviews for this study were conducted nine months after Google, Inc.'s implementation of their revised privacy policy. The interviews revealed that no participants had read the privacy policy and because of the time since the revised

policy was issued, some participants had difficulty remembering if and what they had heard about it. Therefore, a study with participants who had recently read Google, Inc.'s or any other online company's privacy policy would provide an opportunity for comparison of individuals' privacy conceptions and perceptions based on familiarity with the privacy policy. Similarly, a follow-up study of this study's participants on whether or not they have read the March 1, 2012, privacy policy and if their privacy conceptions and perceptions have changed would also allow for a comparison of privacy perspectives.

This study was forthright with its contexts of Gmail and Google which may have made users think about privacy with Google, Inc. more than they might have if they were simply told the study was on privacy. A study where the specific privacy contexts, offline or online, are not disclosed to participants prior to asking the interview questions may provide different perspectives on individuals' privacy, especially in a general sense.

This study could also be replicated with different offline and/or online contexts to reaffirm and/or provide new information on individuals' privacy conceptions and perceptions. This could also uncover additional paradoxes of individuals' privacy beliefs, expectations, and behaviors in the offline and/or online worlds and how individuals' reconcile those dichotomies. These studies could also focus on topics or issues which may have become neglected with technological advancements or societal evolvements.

CHAPTER SIX: CONCLUSION

The issue and notions of privacy can be seen and traced throughout the history of people. While privacy is an implied right, most Americans think it is an explicit right. An interesting, or perhaps ironic, aspect of individuals and privacy is its vague and oppositional nature: most people do not think about privacy until they feel their privacy does not exist. Samuel D. Warren and Louis D. Brandeis (1890) did not write "The Right to Privacy" because they started to notice an erosion of privacy in society or how technological advancements were making privacy invasions easier. Instead, Warren became outraged after news of his wife's parties and his daughter's wedding were in the newspapers. At that time "a lady and a gentleman kept their names and their personal affairs out of the papers," and so he decided to find a legal argument to privacy with the help of his former law partner Brandeis (Prosser, 1960, p. 383). Likewise, privacy lawsuits and regulations do not occur until individuals feel their privacy has been violated and these are complicated by the intricacies of today's technologies that muddle the traditional understandings of privacy. Technologies have and are changing the ways individuals' define and understand privacy. Today technology companies are defining users' privacy through privacy policies while excluding individuals' voices from the privacy definition process.

As this study found, individuals do not have a single definition of privacy for every circumstance, but rather different definitions and expectations of privacy that

depend on the context. While their individual definitions of privacy within each context are not exact matches with those of the other participants, their central idea about privacy is the same. The participants' defined privacy, in general, as maintaining control over their information and expected this definition with Gmail, but not with Google. This distinction between email and search demonstrates that the participants have various privacy definitions and expectations that depend on the situational circumstances. Participants' expectation of privacy with Gmail but not with Google exemplifies the disconnect between their multiple privacy definitions and Google, Inc.'s singular privacy policy. Google, Inc. and other online companies need to consider and incorporate individuals' multiple and contextual privacy conceptions and perceptions when creating privacy definitions through privacy policies if harmony is to be achieved between individuals' rights and technological innovation in today's American Technopoly.

Although it seems unlikely that American society would become that of *1984* or *Brave New World*, the continued growth of technology is taking over the culture we used to know and making our society a "culture [that] seeks its authorization in technology, finds its satisfactions in technology and takes its order from technology" (Postman, 1992, p. 71). While these novels seemed like science fiction when they were written in the first half of the 20th century, they are today's reality. The news media often tailor their messages to maintain influential governmental associations and big businesses relations despite possible disadvantages to citizens, closed-caption cameras and videos capture individuals' activities outside their homes, companies profile individuals, and the government has or can access individuals' information (Huxley, 1932/2006; Orwell, 1949/1977). American society's increasing use of technology is overpowering its

people's voices and redefining individuals' notions of and expected rights to privacy, as exemplified by Google, Inc.'s privacy policy revision on March 1, 2012. If society doesn't make a stand and fight for their culture and values the only question remaining is: Which will the American Technopoly end up resembling more, *1984* or *Brave New World*?

REFERENCES

Alexa. (n.d.). *Google.com site info: Traffic Stats* [Webpage]. Retrieved from http://www.alexa.com/siteinfo/google.com

Bartz, D. (2012, July 31). Google expected to face $22.5 million fine in Safari security workaround, admit no liability. *San Jose Mercury News*. http://www.lexisnexis.com

Best, K. (2010). Living in the control society: Surveillance, users and digital screen technologies. *International Journal of Cultural Studies, 13*, 5–24.

Bomey, N. (2011, October 1). Barnes & Noble CEO: 'We're very sorry your Borders store closed.' *Ann Arbor.com*. Retrieved from http://www.annarbor.com

Bosker, B. (2012, August 10). In Google's privacy settlement, tech giant denies liability (again). *The Huffington Post*. Retrieved from http://www.huffingtonpost.com

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development.* Thousand Oaks, CA: Sage Publications.

Branscomb, A. W. (1994). *Who owns information?: From privacy to public access.* New York, NY: Basic Books.

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*, 77–101.

British Library. (n.d.) *Treasures in full: Magna Carta*. Retrieved April 26, 2013 from http://www.bl.uk/treasures/magnacarta/basics/basics.html

Brownlow, M. (2012, January). *Email and webmail statistics* [Web Article]. Retrieved from http://www.email-marketing-reports.com/metrics/email-statistics.htm

Cain Miller, C. (2012, October 17). *Larry Page defends Google's privacy policy* [Web log]. Retrieved from http://bits.blogs.nytimes.com/2012/10/17/larry-page-defends-googles-privacy-policy/

Chavez, P. (2012, January 31). Changing our privacy policies, not our privacy controls [Web log post]. Retrieved from http://googlepublicpolicy.blogspot.com/2012/01/changing-our-privacy-policies-not-our.html

CNBC. (2009, December 29). Google's Privacy [Video file]. Retrieved from http://video.cnbc.com/gallery/?video=1372176413

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches (Second Edition).* Thousand Oaks, CA: Sage Publications, Inc.

deMarrais, K. (2004). Qualitative interview studies: Learning through experience. In eds. Kathleen deMarrais and Stephen D. Lapan, *Foundations for research: Methods of inquiry in education and the social sciences*. (pp. 51–68) Mahwah, NJ: Lawrence Erlbaum Associates.

Denzin, N. K. & Lincoln, Y. S. (2002). The discipline and practice of qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage handbook of qualitative research (Third Edition) (pp. 1–32).* Thousand Oaks, CA: Sage Publications, Inc.

Dinev, T. & Hart, P. (2004). Internet privacy concerns and their antecedents: Measurement validity and a regression model. *Behaviour & Information Technology, 23,* 413–422.

Google, Inc. (2004). Google gets the message, launches Gmail [Press Release]. Retrieved from http://www.google.com/press/pressrel/gmail.html

Google, Inc. (2012, March 1). *Privacy policy* [Web page]. Retrieved from http://www.google.com/intl/en/policies/privacy/

Google, Inc. (n.d.) *Google Locations* [Web page]. Retrieved from http://www.google.com/about/company/facts/locations

Google, Inc. (n.d.). *Our history in depth* [Web page]. Retrieved from http://www.google.com/about/company/history/

Google, Inc. (n.d.). *Privacy FAQ* [Web page]. Retrieved from http://www.google.com/intl/en/policies/privacy/faq/

Google, Inc. (n.d.). *Top 10 reasons to use Gmail* [Web page]. Retrieved from http://mail.google.com/mail/help/intl/en/about.html

Google, Inc. (n.d.) *Transparency Report* [Web page]. Retrieved from http://www.google.com/transparencyreport/

Google privacy policy: Six European data protection authorities to launch coordinated and simultaneous enforcement actions. (2013, April 2). *Commission nationale de l'informatique et des liberties (CNIL)*. Retrieved from http://www.cnil.fr/english/news-and-events/news/article/google-privacy-policy-six-european-data-protection-authorities-to-launch-coordinated-and-simultaneo/

Google settles StreetView privacy lawsuit. (2013, March 12). *RTT News*. Retrieved from http://www.rttnews.com/2075400/google-settles-streetview-privacy-lawsuit.aspx?type=gn&utm_source=google&utm_campaign=sitemap

Google will pay $22.5 million to settle FTC charges it misrepresented privacy assurances to users of Apple's Safari Internet browser. (2012, August 9). *Federal Trade Commission News*. Retrieved from http://www.ftc.gov/opa/2012/08/google.shtm

Guynn, J. (2013, March 13). Google settles privacy inquiry; A $7-million fine will end a case involving collection of personal data by Street View. *The LA Times*, Business section, Business Desk, part B, p. 2.

Helft, M. (2013). The future according to Google's Larry Page. *Fortune*. Retrieved from http://tech.fortune.cnn.com/2013/01/03/google-larry-page/

Henderson, H. (1999). *Privacy in the Information Age*. New York, NY: Facts on File, Inc.

Hill, K. (2010, November 3). Google Buzz was an $8.5-million disaster. Why can't Google do social? *Forbes*. Retrieved from http://www.forbes.com

Huxley, A. (1932/2006). *Brave New World*. New York, NY: HaperCollins Publishers.

Hollander, J. (2001). The language of privacy. *Social Research, 68*, 5–28.

Joinson, A. N., Reips, U-D., Buchanan, T., & Paine Schoefield, C. B. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction, 25*, 1–24.

Kachhi, D. & Link, M. W. (2009). Too much information: Does the Internet dig too deep? *Journal of Advertising Research, 49*, 74–81.

Kang, C. (2012, January 24). Google announces privacy changes across products; users can't opt out. *The Washington Post*. Retrieved from http://www.washingtonpost.com

Kang, C. (2012, February 9). Group sues, accusing Google of violating FTC privacy pact. *The Washington Post.* Retrieved from http://www.lexisnexis.com

Lessig, L. (2006). *Code version 2.0*. New York, NY: Basic Books.

Library of Congress. (2010, July 30). *Bill of Rights.* Retrieved December 12, 2010 from http://www.loc.gov/rr/program/bib/ourdocs/billofrights.html

Liedtke, M. (2012, August 8). Gmail in search results? That's the latest idea from Google. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com

Lincoln, A. (1863, November 19). *Gettysburg Address*. [Speech]. Retrieved July 4, 2013 from http://myloc.gov/Exhibitions/gettysburgaddress/Pages/default.aspx

Louis Harris & Associates, Inc. & Westin, A. F. (1981). *The dimensions of privacy: A national opinion research survey of attitudes toward privacy.* New York, NY: Garland Publishing, Inc.

Louis Harris & Associates, Inc. & Westin, A. F. (1990). *The Equifax report on consumers in the information age.* New York, NY: Equifax Inc.

Louis Harris & Associates, Inc. & Westin, A. F. (1995). *Equifax-Harris mid-decade consumer privacy survey.* New York, NY: Equifax Inc.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues, 59*, 243–261.

Masiello, B. (2012, January 26). Setting the record straight about our privacy policy changes [Web log post]. Retrieved from

http://googlepublicpolicy.blogspot.com/2012/01/setting-record-straight-about-our.html

Masiello, B. (2012, February 1). Busting myths about our approach to privacy [Web log post]. Retrieved from http://googlepublicpolicy.blogspot.com/2012/02/busting-myths-about-our-approach-to.html

Markoff, J. (2004, March 31). Google planning to roll out e-mail service. *The New York Times*. Retrieved from http://www.nytimes.com

Milne, G. R. & Rohm, A. J. (2000). Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives. *Journal of Public Policy & Marketing, 19,* 238–249.

Miyazaki, A. D. (2008). Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage. *American Marketing Association, 27*, 19–33.

Mohan, M. (2012, April 3). *Over 101 Google products and services you probably don't know* [Web Article]. Retrieved from http://www.minterest.com/60-google-products-services-you-probably-dont-know/

Moore, A. (2008). Defining privacy. *Journal of Social Philosophy, 39*, 411–428.

National Archives & Records Administration. (n.d.) *Bill of Rights*. Retrieved April 26, 2013 from http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html

National Archives & Records Administration. (n.d.) *Magna Carta*. Retrieved April 26, 2013 from http://www.archives.gov/exhibits/featured_documents/magna_carta/

Orwell, G. (1949/1977). *1984*. New York, NY: Signet Classics.

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research*. Advance online publication. doi: 10.1177/0093650211418338

Pember, D. R. & Calvert, C. (2011). *Mass media law* (17th ed.). New York, NY: McGraw-Hill.

Postman, N. (1992). *Technopoly: The surrender of culture to technology*. New York, NY: Vintage Books.

Prosser, W. L. (1960). Privacy. *California Law Review*, *48*, 383–423.

Purcell, K. (2011). *Search and email still top the list of most popular online activities: Two activities nearly universal among adult internet users* (Report). Retrieved from Pew Internet & American Life Project website: http://pewinternet.org/Reports/2011/Search-and-email.aspx

Purcell, K., Brenner, J., & Rainie, L. (2012). *Search engine use 2012: Even though online Americans are more satisfied than ever with the performance of search engines, strong majorities have negative views of personalized search results and targeted ads* (Report). Retrieved from Pew Internet & American Life Project website: http://pewinternet.org/Reports/2012/Search-Engine-Use-2012.aspx

Ramsay, H. (2010). Privacy, privacies and basic needs. *Heythrop Journal, 51,* 288–297.

Regan, P. (2003). Privacy and commercial use of personal data: Policy developments in the United States. *Journal of Contingencies and Crisis Management, 11*, 12–18.

Rubin, H. J. & Rubin, I. S. (1995). *Qualitative interviewing: The art of hearing data.* Thousand Oaks, CA: Sage Publications.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society, 18*, 21–32.

Sullivan, D. (2004, March 30). *Google launches Gmail, free email service* [Web Article]. Retrieved from http://searchenginewatch.com/article/2065293/Google-Launches-Gmail-Free-Email-Service

Swift, M. (2011, March 30). Google: FTC orders 20 years of consumer privacy protections. *Contra Costa Times (California).*Retrieved from http://www.lexisnexis.com

Swift, M. (2012, March 12). Google's moves raise questions about 'don't be evil' motto. *Contra Costa Times (California).* Retrieved from http://www.lexisnexis.com

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy, 38,* 1–22.

The Associated Press. (2012, August 12). Google to include Gmail in search results. *Newsday*. Retrieved from http://www.newyork.newsday.com

Thomas, J. & Harden, A. (2008). Methods for thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, *8*, 45–54.

Turow, J. & Hennessy, M. (2007). Internet privacy and institutional trust: insights from a national survey. *New Media & Society, 9*, 300–318.

Viseu, A., Clement, A., & Aspinall, J. (2004). Situating privacy online: Complex perceptions and everyday practices. *Information, Communication & Society*, *7*, 92–114.

Warren, S. D. & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*, 193–220.

Westin, A. F. (1967). *Privacy and freedom.* Atheneum, NY: The Association of the Bar of the City of New York.

Whitten, A. (2012, January 24). Updating our privacy policies and terms of service [Web log post]. Retrieved from http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html

World Digital Library. (2012, January 23). *Bill of Rights*. Retrieved November 6, 2012 from http://www.wdl.org/en/item/2704/

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology, 58,* 710–722.

APPENDIX A

Google, Inc.'s March 1, 2012 Privacy Policy

This is an archived version of our Privacy Policy. View the current version or all past versions.

Last modified: March 1, 2012

There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.

Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

We've tried to keep it as simple as possible, but if you're not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a long-time user, please do take the time to get to know our practices – and if you have any questions contact us.

Information we collect

We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful or the people who matter most to you online.

We collect information in two ways:

- **Information you give us.** For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.
- **Information we get from your use of our services.** We may collect information about the services that you use and how you use them, like when you visit a website that uses our advertising services or you view and interact with our ads and content. This information includes:
    - **Device information**

      We may collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile

network information including phone number). Google may associate your device identifiers or phone number with your Google Account.

- **Log information**

  When you use our services or view content provided by Google, we may automatically collect and store certain information in server logs. This may include:

  - details of how you used our service, such as your search queries.
  - telephony log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
  - Internet protocol address.
  - device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
  - cookies that may uniquely identify your browser or your Google Account.

- **Location information**

  When you use a location-enabled Google service, we may collect and process information about your actual location, like GPS signals sent by a mobile device. We may also use various technologies to determine location, such as sensor data from your device that may, for example, provide information on nearby Wi-Fi access points and cell towers.

- **Unique application numbers**

  Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

- **Local storage**

  We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.

- **Cookies and anonymous identifiers**

  We use various technologies to collect and store information when you visit a Google service, and this may include sending one or more cookies or anonymous identifiers to your device. We also use cookies and

anonymous identifiers when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites.

How we use information we collect

We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads.

We may use the name you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account so that you are represented consistently across all our services. If other users already have your email, or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo.

When you contact Google, we may keep a record of your communication to help solve any issues you might be facing. We may use your email address to inform you about our services, such as letting you know about upcoming changes or improvements.

We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer. When showing you tailored ads, we will not associate a cookie or anonymous identifier with sensitive categories, such as those based on race, religion, sexual orientation or health.

We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.

We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.

Google processes personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live.

Transparency and choice

People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:

- Review and control certain types of information tied to your Google Account by using Google Dashboard.
- View and edit your ads preferences, such as which categories might interest you, using the Ads Preferences Manager. You can also opt out of certain Google advertising services here.
- Use our editor to see and adjust how your Google Profile appears to particular individuals.
- Control who you share information with.
- Take information out of many of our services.

You may also set your browser to block all cookies, including cookies associated with our services, or to indicate when a cookie is being set by us. However, it's important to remember that many of our services may not function properly if your cookies are disabled. For example, we may not remember your language preferences.

Information you share

Many of our services let you share information with others. Remember that when you share information publicly, it may be indexable by search engines, including Google. Our services provide you with different options on sharing and removing your content.

Accessing and updating your personal information

Whenever you use our services, we aim to provide you with access to your personal information. If that information is wrong, we strive to give you ways to update it quickly or to delete it – unless we have to keep that information for legitimate business or legal purposes. When updating your personal information, we may ask you to verify your identity before we can act on your request.

We may reject requests that are unreasonably repetitive, require disproportionate technical effort (for example, developing a new system or fundamentally changing an existing practice), risk the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup tapes).

Where we can provide information access and correction, we will do so for free, except where it would require a disproportionate effort. We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

Information we share

We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances apply:

- **With your consent**

  We will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.

- **With domain administrators**

  If your Google Account is managed for you by a domain administrator (for example, for Google Apps users) then your domain administrator and resellers who provide user support to your organization will have access to your Google Account information (including your email and other data). Your domain administrator may be able to:

  - view statistics regarding your account, like statistics regarding applications you install.
  - change your account password.
  - suspend or terminate your account access.
  - access or retain information stored as part of your account.
  - receive your account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.
  - restrict your ability to delete or edit information or privacy settings.

  Please refer to your domain administrator's privacy policy for more information.

- **For external processing**

  We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

- **For legal reasons**

  We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

  - meet any applicable law, regulation, legal process or enforceable governmental request.
  - enforce applicable Terms of Service, including investigation of potential violations.
  - detect, prevent, or otherwise address fraud, security or technical issues.
  - protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.

We may share aggregated, non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services.

If Google is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

Information security

We work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular:

- We encrypt many of our services using SSL.
- We offer you two step verification when you access your Google Account, and a Safe Browsing feature in Google Chrome.
- We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.
- We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

Application

Our Privacy Policy applies to all of the services offered by Google Inc. and its affiliates, including services offered on other sites (such as our advertising services), but excludes services that have separate privacy policies that do not incorporate this Privacy Policy.

Our Privacy Policy does not apply to services offered by other companies or individuals, including products or sites that may be displayed to you in search results, sites that may include Google services, or other sites linked from our services. Our Privacy Policy does not cover the information practices of other companies and organizations who advertise our services, and who may use cookies, pixel tags and other technologies to serve and offer relevant ads.

Enforcement

We regularly review our compliance with our Privacy Policy. We also adhere to several self regulatory frameworks. When we receive formal written complaints, we will contact the person who made the complaint to follow up. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that we cannot resolve with our users directly.

Changes

Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of privacy policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.

Specific product practices

The following notices explain specific privacy practices with respect to certain Google products and services that you may use:

- Chrome and Chrome OS
- Books
- Wallet

APPENDIX B

Interview Script

INTERVIEW SCRIPT

Thank you for agreeing to speak with me today.

The purpose of this interview is to learn about and understand your thoughts and ideas about privacy as a Google and/or Gmail user. Since the goal of this study is to understand your conceptions and perceptions of privacy there are no right or wrong responses.

This discussion will be guided by your responses so if you do not wish to answer a question or continue with the interview please let me know and we will discuss another response or end the interview.

The interview can last between thirty minutes and two hours, depending on our discussion, and will be audio-recorded to make sure that it is recorded accurately.

Do you have any questions for us before we begin?

QUESTIONS

What is privacy to you? Define privacy.

What is privacy to you when using Gmail, Google, and/or Googling in Gmail? Define privacy with Gmail, Google, and/or Googling in Gmail.

How long have you used Gmail and/or Google?

Do you have an account with Google, Inc.?

Follow-up questions regarding and expanding upon participants' comments to be asked.

The final interview questions for each participant will be:

Have you read Google, Inc.'s new (March 1, 2012) privacy policy?

Do you feel you understand the privacy policy?

Tell me about the privacy policy. Could you summarize the policy?

Is there anything I haven't asked you about privacy with Google, with Gmail, or with Google, Inc. that you would like to share?