June 2017

# Privacy vs. Security: Fear appeals, terrorism and the willingness to allow increased government surveillance

Angela Marie Rulffes
*Syracuse University*

**Abstract**

This study investigates the relationship between fear and privacy by using the Extended Parallel Process Model (EPPM) to examine whether there is an association between fear appeals and the willingness to allow increased governmental surveillance of online and phone communications. Research suggests that, in the United States, privacy is important. Moreover, courts have inferred privacy rights in the U.S. Constitution, including protection from intrusions by the government. However, the threat of terrorism is also very real. There are indications that some people may be willing to allow intrusion by the government if it means keeping them safe. This study uses an experimental method to determine whether the fear of terrorism is stronger than the need to keep private communications secure from the government. EPPM is a dominate theory in the area of fear appeals and persuasion. Scholars indicate that the EPPM can predict whether a persuasive message will be successful based on the levels of threat and efficacy. The underlining assumption of the theory is that if a person feels fear, that person will take some sort of action to alleviate the fear. EPPM research suggests that, in order to persuade, a fear appeal message must contain language that accentuates a high threat and high efficacy to combat the threat. According to the theory, if a person perceives a high threat and high efficacy (*i.e.,* feels he or she has the ability to overcome the threat by taking the action proposed in the message), that person will be persuaded by the message. EPPM is used primarily in the field of health communication; however, this study takes a unique route by using EPPM to study attitudes and behaviors toward terrorism and privacy rights policies. This study used terrorism as the threat and offered two separate efficacy options. The first was allowing increased government surveillance, and the second was individual reporting of suspicious activity to police. This study found no support for the EPPM hypotheses, meaning there was no indication that participants

who read the fear appeal containing the high threat and high efficacy options were persuaded by the message. However, the results did offer evidence that a high pre-existing perception of the threat could make a fear appeal ineffective. The perceived terrorism threat severity level for all of the experimental groups, including the control group, were high, which left little room for the threat to be increased using a fear appeal. EPPM proposes that, in order to be persuaded, the perceived efficacy felt by the reader of the message must be able to surpass the perceived threat. In this case, it is likely that the perceived threat of terrorism is so high that the efficacy options provided could not overcome the threat. Moreover, the results provided evidence that type of efficacy offered in the fear appeal message is important.

This study also extends EPPM research by determining if there is a relationship between cognitive dissonance and rejection of a fear appeal message. Cognitive dissonance refers to inconsistencies between an individual's beliefs and actions. The theory proposes that if an individual has an inconsistency in her beliefs and behaviors, it can lead to discomfort. The individual will want to alleviate the discomfort by reducing the dissonance, which could mean either changing beliefs or behaviors to make them consistent.

This study proposed that the amount of dissonance a person feels when reading a fear appeal may affect whether the person accepts or rejects the message. The results showed that cognitive dissonance is a predictor of message rejection. The higher the amount of cognitive dissonance the participant felt when reading the fear appeal message, the more likely that participant was to reject the message. In fact, the results indicated that cognitive dissonance is a better predictor of message rejection than perceived threat and perceived efficacy combined. This finding suggests that cognitive dissonance should be considered when drafting a fear appeal message and that it should be included as a variable in the EPPM theoretical model.

Finally, this study investigated the relationship between cognitive dissonance and the privacy paradox theory. The privacy paradox theory refers to an inconsistency between a person's beliefs and behaviors about privacy. The results indicated that there is a relationship between dissonance and the privacy paradox.

# Privacy vs. Security: Fear appeals, terrorism and the willingness to allow increased government surveillance

by

Angela M. Rulffes

B.S., Plattsburgh State University, 2002
M.S., Syracuse University, 2003
J.D., Cleveland-Marshall College of Law, 2009

Dissertation
Submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Mass Communication.

Syracuse University
May 2017

# Table of Contents

## Case Index

# Chapter 1: Introduction

In the United States, privacy is considered an important constitutional right, and there are indications that citizens value protection against intrusions by the government. In June 2013, when Edward Snowden released information about PRISM, a U.S. government surveillance program, there was public concern about possible privacy violations (Florek, 2013; Palmer, 2013). More recently, issues of privacy and governmental intrusion surfaced when the Federal Bureau of Investigation sought to gain access to a locked iPhone (Benner & Lichtblau, 2016). In both the PRISM and iPhone cases, the government indicated that its concern was national security and protection from terrorist attacks (Florek, 2013; Palmer, 2013; Selyukh & Domonoske, 2016). The government has an expectation that the interception of terrorist communication will help protect U.S. citizens (Florek, 2013).

Although privacy from governmental intrusion is an important issue, the threat of terrorism is also very real. In some instances, people may be willing to allow intrusion by the government if it means keeping them safe. This study examines the effects of the fear of terrorism on people's attitudes toward governmental surveillance. The purpose of this study is to test the Extended Parallel Process Model (EPPM) to discover if fear appeals will cause people to be more likely to give up privacy rights and allow intrusive governmental surveillance in order to ensure national security. Moreover, this study will examine the extent to which cognitive dissonance regarding the fear appeal affects how people react to it.

In 1928, Supreme Court Justice Louis Brandeis said in his dissenting opinion that the right to be let alone is "the most comprehensive of rights and the right most valued by civilized men" (*Olmstead v. United States*, p. 478). Nearly 40 years later, the U.S. Supreme Court determined that the Fourth Amendment includes a right to privacy in *Katz v. United States*

(1967). Since that time, there have been many lawsuits arguing that governmental intrusion has led to violation of constitutional privacy rights.

In June 2013, leaks by Edward Snowden led to the discovery of three NSA surveillance programs, which have since led to a variety of law suits. One of the programs, PRISM, was designed by United States and British governments to gather intelligence pertaining to terrorist activities in an effort to enhance national security (Blass, 2014; Florek, 2013). According to reports, the NSA and the Federal Bureau of Investigation (FBI) gained access to the central servers of significant media and social networking companies including Facebook, Google and Apple (Blass, 2014; Florek, 2013). Through this access, the government was able to extract information such as photos, emails, connection logs, audio and video chats, and other stored data (Blass, 2014; Florek, 2013). A second program involved the NSA's upstream collection of communications (Blass, 2014). This program allowed the NSA to monitor and seize internet communications without a warrant (*Wikimedia v. NSA*, 2016). Because this program allowed for the bulk capturing, copying and searching of the content of international and domestic internet communications, there were people who argued that upstream surveillance violated privacy rights (*Wikimedia v. NSA*, 2016). These concerns about privacy violations have led legal challenges to the NSA's program (*Wkimedia v.* NSA, 2016). A third program code-named XKeyscore collected the information that the NSA was mining and aggregated it into a database in order to search and analyze the information (Blass, 2014; Florek, 2013).

These surveillance programs were authorized under the 2008 Amendments to the Foreign Intelligence Surveillance Act (FISA) of 1974, which allowed the NSA to gather foreign intelligence information by targeting people located outside of the United States (FISA, 2008; Florek, 2013). The "Limitations" section of the statute states that the government cannot

"intentionally target any person known at the time of acquisition to be located in the United States" and cannot "intentionally acquire any communication" where the sender and all recipients "are known at the time of acquisition to be locate in the United States" (FISA, Section 702, 2008; Florek, 2013). However, the language of the law leaves open the possibility that the NSA many collect communications of U.S. citizens when they are receiving or sending communications to an NSA target (Eoyang, 2016). There has been much debate over whether the PRISM, Upstream surveillance, and XKeyscore programs violated U.S. citizens' Fourth Amendment privacy rights. For example, after *The Guardian* and *The Washington Post* broke the story regarding the NSA's surveillance programs, the American Civil Liberties Union (ACLU) filed two lawsuits. The first, *ACLU v. Clapper* (2015), challenged the NSA's ability to mass collect phone records of U.S. citizens (ACLU v. Clapper – Challenge to NSA, 2015). The second suit, *Wikimedia v. NSA* (2016), argued that the NSA's mass interception of U.S. citizens' international online communications was unconstitutional (Wikimedia v. NSA – Challenge to Upstream Surveillance, 2015). In *ACLU v. Clapper* (2015), the Court of Appeals for the Second Circuit found that the NSA's collection of phone records was not authorized by Section 215 of the Patriot Act, which the government had cited as statutory legal basis for the program. The court did not determine whether there was a privacy violation under the Fourth Amendment (*ACLU v. Clapper*, 2015). The *Wikimedia* case was dismissed by the U.S. District Court for the District of Maryland and as of this writing is under appeal in the U.S. Court of Appeals for the Fourth Circuit (Wikimedia v. NSA – Challenge to Upstream Surveillance, 2015). It is important to distinguish data collections from content collection. *ACLU v. Clapper* was arguing that the collection of phone records, consisting primarily of phone numbers dialed and received, was unconstitutional. In that case, there were no allegations that the actual content of phone calls was

being overheard using surveillance. *Wikimedia v. NSA* also involves the collection of data; however, the ACLU also argued that the NSA copies the communications it collects and "reviews the copied communications – including their full content – for instances of" email addresses, phone numbers and other identifiers for NSA targets (*Wikimedia v. NSA*, 2016, p. 13). While data collection is an issue, there is more of a concern with the capture and search of the content of communications. However, top security researcher Bruce Schneier, a fellow at Harvard's Berkman center, said that metadata contains highly sensitive information. Schneier, along with fellow computer and data science experts, joined an *amicus* brief on behalf of the ACLU in the *Clapper* case because of his concerns about the government's collection of telephone metadata (Schneier, 2014). Schneier states that "metadata equals surveillance data, and collecting metadata on people means putting them under surveillance" (Scheiner, 2014).

More recently, issues of privacy and governmental intrusion came up when the Federal Bureau of Investigation (FBI) sought to gain access to a locked iPhone (Benner & Lichtblau, 2016). According to an article in the *New York Times*, Apple argued that this action could have negative ramifications on the right to privacy against governmental intrusion (Benner & Lichtblau, 2016). After the murder of 14 people in San Bernardino, California in December, 2015, the FBI obtained an iPhone used by one of the attackers (Benner & Lichtblau, 2016; Selyukh & Domonoske, 2016). The issue, however, was that the phone was encrypted (Benner & Lichtblau, 2016; Selyukh & Domonoske, 2016). The only way for the FBI to access the information on the phone would be get around the phone's passcode security feature; however, Apple refused to help the government because the company said such a tool could be used to breach other electronic devices, which could allow the government to violate peoples' privacy (Benner & Lichtblau, 2016; Selyukh & Domonoske, 2016).

The particular interest of this study is to discover if a fear appeal might persuade people to allow the government to intrude on their personal lives. Fear can be a strong motivator. Indeed, studies indicate that fear can lead people to change their attitude and behavior (Rogers, 1983; Witte, 1994; Witte, 1994; Maloney, Lapinski, & Witte, 2011). Currently, EPPM is one of the predominate theories in this area. Scholars indicate that the theory can predict whether a persuasive campaign will be successful based on the levels of threat and efficacy (Witte, 1994; Witte, 1994; Maloney, Lapinski, & Witte, 2011). EPPM suggests that people process fear appeals both cognitively and emotionally and uses these variables to determine whether a persuasive campaign will be successful (Witte, 1994). Scholars often use EPPM to study the effects of health communications and motivations to live healthier lifestyles. There are few EPPM studies that focus on non-health-related issues and none that examine the threat of terrorism. This study takes a unique route by using EPPM to study attitudes and behaviors toward terrorism and privacy rights policies. Moreover, though EPPM studies have varied the level of efficacy, none have attempted to investigate and compare two different efficacy options in response to the same threat. This study addresses gaps in the research by using EPPM to examine attitudes and behaviors toward terrorism. In addition, no studies have examined whether cognitive dissonance might play a role in predicting message acceptance and message rejection. This study addresses that gap in the research as well.

Social scientists and psychologists tend to focus studies about privacy on issues of boundary building (Altman, 1976; Petronio, 2002) and self-disclosure (Trepte & Reinecke, 2011, Westin, 2003). These scholars have proposed theoretical frameworks to help understand how people determine what should be private and how they control what information they share with others. In addition, legal scholars have investigated the conceptualization of privacy (Solove,

2002; Solove, 2008; Westin, 2003) and examined it in connection with data security (Schwartz, 2013; Henry, 2015; Bambauer, 2013) and contextual integrity (Nissenbaum, 2004). These studies attempt to understand and define privacy within both the legal sense and in the examination of human behavior. However, there are no studies that investigate whether fear appeals, such as a terrorist threat, will make it more likely for people to allow governmental access to communications that are generally considered private.

Privacy is not a term that can easily be defined. Various scholars have attempted to find an all-encompassing definition for privacy. For example, it can be viewed as the right to control interpersonal boundaries (Altman, 1976; Petronio, 2002), thoughts and reputation (Solove, 2002), and personal information (Gormley, 1992). Daniel Solove suggests that privacy can mean the "solitude in one's home" and "freedom from surveillance" (Solove, 2002, p. 1089). He also argues that rather than trying to find a single comprehensive definition of privacy, scholars should instead "explore what it means for something to be private contextually by looking at particular practices" (Solove, 2002, p. 1093). Helen Nissenbaum (2004) also suggests that privacy must be evaluated based on context. Her theory, contextual integrity, suggests that what, how and when information is shared is critical in determining whether there has been a privacy violation. Nissenbaum's work focuses particularly on new communication technology because using technology in a way that is not generally foreseeable by the public could lead to a breakdown in contextual integrity, which could further lead to a privacy violation (Nissenbaum, 2004). Nissenbaum (2004) argues that public surveillance often results in a violation of contextual integrity.

Privacy and surveillance are both important topics because online privacy is a significant concern for people in the United States. A Pew Research Center study found that 50 percent of

internet users are concerned about the degree to which their personal information is available online (Rainie, 2013). Moreover, people are increasing their use of encryption to keep online information safe. In a 2016 report, Bruce Schneier and his colleagues conducted a survey of encryption products and found 865 of these products worldwide. The report indicated that the United States produced the most products at 304, while Germany came in second at 112, and the United Kingdom came in third at 54 (Schneier, Seidel, & Vijayakumar, 2016). In addition, reactions to the PRISM program and to the FBI's iPhone request make it clear that the violations of privacy rights by the government are not welcome (Benner & Lichtblau, 2016; Selyukh & Domonoske, 2016; Wikimedia v. NSA – Challenge to Upstream Surveillance, 2015). A 2016 Reuters' poll indicated that "a majority of Americans do not want the government to have access to their phone and Internet communication, even if it is done in the name of stopping terror attacks" (Finkle, 2016). This study extends current research by going beyond an analysis of an individual's understanding of privacy and boundary construction, to examine the extent to which fear appeals will lead to an acceptance of enhanced surveillance techniques.

Chapter 2 of this study is the Literature Review, which discusses privacy rights in the United States and the theoretical conceptualization of privacy. Chapter 3 offers an examination of the theoretical foundation for this study. Chapter 4 contains a thorough description of the experimental method. Chapter 5 contains the experiment results. Chapter 6 provides a discussion of the results and limitations, and Chapter 7 offers suggestions for future research and the conclusion.

# Chapter 2: Literature Review

The focus of this study is fear appeals and willingness to allow increased governmental surveillance. At the heart of governmental intrusion issues in the United States is privacy law. When people in the United States pushed back against programs like PRISM and FBI access to encrypted iPhone information they based their arguments on the constitutional right of privacy. Thus, when discussing governmental intrusion and surveillance, it is important to recognize the relationship between those issues and privacy.

This Literature Review is divided into two parts. The first part provides a historical review of privacy rights in the United States, focusing on tort law and Fourth Amendment rights. Part 1 also discusses the effect technology has had on privacy rights and data security. The second part offers a review of the various theoretical conceptualizations of privacy.

## Part 1: Privacy rights then and now

It is important to recognize that the word "privacy" is not expressly stated in the U.S. Constitution. There is no section or amendment stating that U.S. citizens have a constitutional right to privacy. Instead, the right to privacy has been inferred through the courts' interpretations of the Constitution. Privacy rights were initially proposed by Louis Brandeis and Samuel Warren in a Harvard Law Review article in 1890 (Warren & Brandeis, 1890). When Warren and Brandeis wrote their article, they were concerned about newspapers publishing private facts (Warren & Brandeis, 1890). They believed that media were invading peoples' personal lives and proposed that "the protection of the person" should include the "right to be let alone" (Warren & Brandeis, 1890, p. 198). They viewed privacy as a right that every individual inherently possessed, allowing that person to control "to what extent his thoughts, sentiments, and emotions shall be communicated to others" (Warren & Brandeis, 1890, p. 198; Gormley, 1992). Warren

and Brandeis urged the courts to recognize a cause of action for the invasion of privacy. Later, after Brandeis became a Justice in the U.S. Supreme Court, he noted in his dissenting opinion in *Olmstead v. United States* (1928) that "the right to be let alone … [is] the most comprehensive of rights and the right most valued by civilized men" (*Olmstead*, p. 478). In *Olmstead*, the plaintiffs alleged that the government violated their Fourth Amendment rights by wiretapping their private telephones and using the conversations as evidence in a criminal trial. The Supreme Court found that there was no violation of constitutional rights in that case.

Over time, the courts began to expand their decisions in order to recognize a right to privacy. In fact, multiple privacy rights were formed as the result of the Warren and Brandeis article (Gormley, 1992). These privacy rights include tort privacy, Fourth Amendment privacy, privacy contained in state constitutions, First Amendment Privacy, and "Fundamental-Decision Privacy" (Gormley, 1992, p. 2). This study focuses on two of those distinct privacy rights. The first is tort privacy and the second is privacy against unreasonable governmental intrusion. These two rights will be explained in detail below.

*Tort Privacy*

Not long after Brandeis and Warren published their article, the Supreme Court of Georgia tentatively recognized a right of privacy in *Pavesich v. New England Life Ins. Co.* (1905). The court stated that the right to privacy is "derived from natural law" and "guaranteed" through the U.S. Constitution "in those provisions which declare that no person shall be deprived of liberty except by due process of law" (*Pavesich*, 1905, p. 71). Nonetheless, the right to privacy did not come into fruition overnight. Moreover, when it finally did take root, there was not a single privacy tort definition (Prosser, 1960). Instead, through state common law and statutory law, Brandeis and Warren's proposed right evolved into four distinct torts: intrusion upon an

individual's solitude or private affairs; public disclosure of embarrassing facts; placing an individual in a false light; and appropriation of a person's name or likeness (Prosser, 1960; Gormley, 1992).

In 1960, William Prosser authored a law review article providing an in-depth overview of the four privacy torts. Intrusion upon a person's solitude involves physical intrusion (*i.e.* entering someone's home or eavesdropping) (Prosser, 1960). In order for there to be violation, there must be an offensive or objectionable intrusion on a private matter (Prosser, 1960). According to Prosser (1960), this particular tort was used to "fill in the gaps left by trespass, nuisance, and the intentional infliction of mental distress" (Prosser, 1960, p. 392). Public disclosure of embarrassing facts has three elements. There must be a (1) public disclosure of (2) private facts, (3) the release of which would be offensive or objectionable to a reasonable person (Prosser, 1960). For this tort, private facts would include information regarding sexual orientation, financial condition, medical information and domestic problems (Trager, Russonmanno, Ross, & Reynolds, 2013). The tort of false light involves the intentional or reckless public disclosure of an alleged fact about an individual that is not actually true (Prosser, 1960). The information must be highly offensive and something that a reasonable person would object to (Prosser, 1960). This tort is closely related to defamation (Prosser, 1960). Finally, appropriation is the use of an individual's name or likeness without her consent and to the benefit of the person using the likeness (Prosser, 1960). This tends to be the unauthorized use of a celebrity's likeness without monetary compensation. The interests protected through this tort is primarily proprietary in nature (Prosser, 1960).

The majority of the four torts require the publication of private information or personal likeness, which involves an affirmative action to make the information public through the use of

communication. Intrusion is unique in that there does not need to be a publication. However, because it involves an objectionable intrusion on a private matter (Prosser, 1960), there is still an affirmative action taken to acquire the information.

Unlike the federal constitution, some state constitutions expressly recognize a general right to privacy. This recognition, however, did not take place until the late 1960s and 1970s – after the U.S. Supreme Court decided *Katz* (Gormley, 1992). Article 1, Section 1 of the California Constitution provides that people have inalienable rights that include "obtaining safety, happiness, and privacy." Alaska, Arizona, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina and Washington also have constitutional provisions providing privacy protection. In addition, many states have passed statutory laws bestowing privacy rights to individuals that are sometimes broader than those afforded through common law.

*Protection from governmental intrusion*

Nearly forty years after *Olmstead* (1928), the U.S. Supreme Court held in *Katz v. United States* (1967) that a privacy right in relation to governmental intrusion was included in the U.S. Bill of Rights. Specifically, the Court indicated that privacy can be inferred from the language of the Fourth Amendment, which states that people have the right to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" (*U.S. Const. amend. IV*). In *Katz v. United States*, the Court decided that the Fourth Amendment protects an individual's "privacy against … government intrusion" (*Katz*, 1967, p. 350).

Interestingly, it was the advent of new, more efficient and accessible technology that led to the Court's decision to recognize a Fourth Amendment right to privacy (Gormley, 1992). In *Katz*, the FBI used an electronic device to listen in on and record Charles Katz's telephone conversation in a public telephone booth. Katz was using the phone to conduct illegal gambling

activities, and, after listening in on his conversations, the government charged and convicted him of violations to federal statutory law (*Katz*, 1967). Katz appealed his conviction and it subsequently made its way to the U.S. Supreme Court. In deciding the case, the Court found that the government's actions "violated the privacy upon which [Katz] justifiably relied … and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment" (*Katz*, 1967, p. 353). In addition, the Court offered further explanation regarding privacy rights. It found that the Fourth Amendment "protects people, not places" (*Katz*, 1967, p. 351). Therefore, even if a person is within the privacy of his own home there will be no Fourth Amendment protection if he knowingly discloses private information to the public (*Katz*, 1967). On the other hand, "What [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected" (*Katz*, 1967, p. 351).

In his concurrence to *Katz* (1967), Justice Harlan proposed a two-prong privacy test that courts continue to use today in cases concerning governmental intrusion. The test states that, in order to have a privacy interest, an individual must show that: 1) he or she has an actual expectation of privacy; and 2) society would recognize that expectation as reasonable (*Katz v. United States*, 1967). Ten years later, in *United States v. Chadwick* (1977), the Court reiterated that the protection afforded by the Fourth Amendment is not limited to dwellings. Instead, it is the individual who is protected from unreasonable governmental intrusion (*Chadwick*, 1977). In *Chadwick*, the respondents were arrested by federal agents after they disembarked a train and loaded their double-locked footlocker into the trunk of their car (*Chadwick*, 1977). The Court found that the respondents had a reasonable expectation of privacy in the footlocker and that the government needed a warrant in order to search it (*Chadwick*, 1977). In its decision, the Court relied heavily on the privacy test proposed in *Katz*.

*Technology, new media and privacy*

With the fast pace of technological advancements and the advent of the Internet and new media, privacy rights continue to evolve. In a 2001 case, the Supreme Court found that if the government conducts a search using a technological device that is not generally used by the public, a warrant is required (*Kyllo v. United States*, 2001). In *Kyllo* (2001), the federal government used a thermal imaging device to find out if Danny Kyllo was growing marijuana in his home. By using the device, the federal agents were able to detect the heat from the lamps used to grow the plants without having to enter Mr. Kyllo's home (*Kyllo*, 2001). The Court found that using the thermal-detection technology constituted a Fourth Amendment search and violated Kyllo's rights. On the other hand, the use of technology to gather information is not always a privacy violation, particularly when the information being sought by the government is data, rather than the content of a communication. In *Smith v. Maryland* (1979), the police were trying to catch a man who was placing harassing phone calls. The police asked the phone company to install a pen register in order to record the phone numbers dialed by the man on his home phone (*Smith v. Maryland*, 1979). Relying on *Katz*, the Supreme Court found that the use of a pen register does not constitute a Fourth Amendment search because people do not have a reasonable expectation of privacy in the numbers they dial (*Smith v. Maryland*, 1979). A critical aspect of this case is that phone numbers, and not content from the actual phone calls, were being recorded. It is also important to note that the *Smith v. Maryland* (1979) Court also found that a person's expectation of privacy in information can be extinguished when that information is shared with a third party. In that case, the Court determined that when a person dials a phone number, the person is voluntarily providing that information to the phone company in order to

use the phone company's services (*Smith v. Maryland*, 1979). Once that information is shared with the phone company, the dialer can no longer control what the phone company does with that information (*Smith v. Maryland*, 1979).

Courts have found that the use of eavesdropping technology without a warrant can be a violation of the Fourth Amendment (*Berger v. New York*, 1967) and that people generally have an expectation of privacy in their personal computer (*U.S. v. Lifshitz, 2004; U.S. v. Buckner*, 2007; U.*S. v. Heckenkamp*, 2007). Moreover, people also have a reasonable expectation of privacy in the information contain on their cell phones. In *Riley v. California* (2014), Riley was pulled over for a traffic stop and arrested for illegally carrying a weapon. At the time of his arrests, the police seized and searched his cell phone (*Riley v. California*, 2014). The Supreme Court determined that the police cannot search the cell phone of an arrested person without first obtaining a warrant (*Riley v. California*, 2014). The Court likened cell phones to a miniature computer, which can carry a significant amount of personal, private data about an individual (*Riley v. California*, 2014).

The popularity of the Internet has led to additional privacy concerns. Social media sites like Facebook collect personal information from users and then provide it to advertisers, which results in personalized advertisements (Tucker, 2014). A survey conducted by the Pew Research Center indicated that 57 percent of all American adults use Facebook (Smith, 2014). Moreover, looking just at American adults who use the Internet, 73 percent of them use at least one type of social networking site, and 71 percent of them use Facebook (Duggan & Smith, 2013). Facebook recently expanded how it utilizes user data for advertisement purposes (Miners, 2014; Vara, 2014). This expansion has caused many to raise questions about privacy issues while using the platform, with some arguing that this expansion significantly increases the intrusion on users'

private information (Miners, 2014). Over the past few years, Facebook users have criticized the company for its privacy policy and manipulation of newsfeeds (Farr & Oreskovic, 2014). The company published an apology to its users in October 2014 for a secret experiment it conducted in which it changed users' news feeds to show them either low levels of positive or negative posts in order to determine if the type of posts a person reads can affect that person's emotional state (Rushe, 2014). Moreover, there have been criticisms from users about Facebook's privacy options, and the media has been covering complaints about the platform's privacy issues for years (Sydell, 2012). Additionally, in November 2014, Facebook said that it had been receiving increasing numbers of requests by various governments for user information ("Facebook says government," 2014).

There is some debate and scholarly research regarding whether social media sites like Facebook are actually private (Burkell, Fortier, Wong, & Simpson, 2014). Courts have found that, under some circumstances, the government can access Facebook posts without violating the user's constitutional privacy rights regardless of whether the user has privacy settings in place (*Palmieri v. United States*, 2014; *United States v. Meregildo*, 2012). For example, multiple federal courts have determined that "when a Facebook user allows 'friends' to view his information, the government may access that information through an individual who is a 'friend' without violating the Fourth Amendment" (*Palmieri v. United States*, 2014, p. 11; *United States v. Meregildo*, 2012). In *Palmieri v. United States* (2014), plaintiff Matthew Palmieri, who was a former contractor for the United States, sued the government after his security clearance was revoked following a federal investigation into his online activities. During its investigation, the government accessed information contained in Palmieri's Facebook account without his permission (*Palmieri*, 2014). Specifically, Palmieri alleged that one of his Facebook "friends,"

who had permission to access his wall, obtained information about him and shared it with federal investigators. The U.S. District Court for the District of Columbia determined that the government did not violate Palmieri's constitutional rights because it was the Facebook friend and not the government that initially accessed and shared the information (*Palmieri*, 2014).

Courts have also determined that although an individual has a reasonable expectation of privacy in information contained in his or her computer, that expectation can be lost if the individual shares the information with the public using a website (*Palmieri v. United States*, 2014; *United States v. Meregildo*, 2012). In the case of *United States v. Meregildo* (2012), the court indicated that a Facebook user cannot expect his friends to keep the information on his wall private and that he shared posts with his friends at his own peril. The court also found that when a Facebook user posts information to the public, the user's postings do not have Fourth Amendment protection (*Meregildo*, 2012). However, somewhat confusingly, the court also stated that "postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected" (*Meregildo*, 2012, p. 525). This could illustrate the courts' inability or refusal to strictly define Facebook as private or public. Facebook and other social media sites change their privacy and security settings often in order to deal with new threats. As communication technology continues to evolve, it is likely that courts will be required to determine how these changes affect privacy rights.

*Privacy, governmental surveillance and terrorism*

Law enforcement has often utilized surveillance and eavesdropping techniques in order to gather intelligence concerning illegal activities in the United States. In the case of *Berger v. New York* (1967), the U.S. Supreme Court found that the use of eavesdropping technology without a warrant violated the Fourth Amendment. In *Berger* (1967), the government argued that

electronic interception of communications is necessary to combat organized crime. Similar arguments have been made today regarding electronic surveillance to fight terrorism. For example, at the beginning of the 2016 U.S. elections, then-presidential candidates Hillary Clinton and Donald Trump called "for a beef-up for government surveillance programs in the wake of terrorist attacks in Paris and San Bernardino, California" (McCarthy, 2015). However, around the same time, security experts were arguing that surveillance cannot stop terrorism (Brooks, 2015; Schneier, 2016).

Because technology evolves quickly and continuously, the nature of the relationship between privacy and national security is dynamic and in a constant state of flux. With the advent of smart phones and new media technology, the ability to communicate with others and store data has advanced considerably. Along with these advances come new avenues for government surveillance and fresh concerns about privacy. In addition, surveillance laws are repealed, revised, or amended frequently, often due to concerns about privacy.

Though the government has used surveillance in the name of national security for a long time, the significant changes came after September 11, 2001. After the 2001 terrorist attacks, the U.S. government began a more intense stance on surveillance and the use of surveillance to combat terrorism. A little over a month after the attacks, Congress passed the PATRIOT Act. Provisions of the PATRIOT Act provided the government with unprecedented power to use surveillance to fight terrorism (Christensen, 2006). The Act categorized terrorism in a way that allowed the government to investigate the suspicion of domestic terrorism offenses through the use of wiretaps and searches of electronic communications (Christensen, 2006; Napolitano, 2013). The law made it easier for the government to obtain search and wiretap warrants (Christensen, 2006; Napolitano, 2013). Around the same time, President Georgia W. Bush

created the Terrorism Surveillance Program (codenamed “Stellar Wind”), which allowed the NSA to unconstitutionally gather bulk telephone and internet data of U.S. citizens (Napolitano, 2013; Schneier, 2015). Information about Stellar Wind was leaked in 2004 by a former Justice Department attorney (Schneier, 2015; Zetter, 2013). The program was supposedly ended in 2011 (Zetter, 2013); however, security experts such as Schneier suggest that the NSA did not stop collecting email metadata, but rather, “just cancelled one particular program and changed the legal authority under which they collected it” (Schneier, 2015). Schneier suggests that the FISA Act of 2008 was a “replacement source for the data collection,” which authorized Internet companies and service providers to give the government bulk data collected from the U.S. public (Napolitano, 2013). The PRISM program, later leaked to the public by Edward Snowden, was formulated from the authority of 2008 FISA amendments (Napolitano, 2013). Civil rights organizations argued that Stellar Wind and PRISM violated U.S. citizens’ privacy rights (Christensen, 2006; Napolitano, 2013). Section 215 of the Patriot Act, which granted the government broad access to U.S. citizen’s communications was significantly restricted under the USA Freedom Act, enacted in 2015 (Recommendations Assessment Report, 2016). However, Section 702, which enabled the PRISM project and Upstream surveillance, remained intact.

There are individuals in the government who argue surveillance is necessary in order to protect the public from terrorism. In 2013, then National Security Agency Director, Keith Alexander, told the House Intelligence Committee that PRISM helped to prevent approximately 50 terrorist activity plots (Nelson, 2013). Mike Rogers, the former chairman of the House Intelligence Committee, said in 2015 that the National Security Agency (NSA) needs to have broad powers to monitor international phone calls in order to fight ISIS and stop terrorist recruitment in the United States (Carroll, 2015). Hillary Clinton told *Time* in 2015 that

monitoring of social media and increased surveillance were necessary to stop ISIS (Frizell, 2015).

Of course, when it comes to an increase in electronic surveillance, there is always a question of whether someone's privacy is violated. Indeed, the U.S. Supreme Court stated in *Berger*, that "The fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual; …indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments" (p. 62, quoting *Lopez v. United States*, 373 U.S. 427 (1963)).

Civil liberties advocates argue that government surveillance infringes on U.S. citizen's privacy rights. In fact, the ACLU has filed multiple lawsuits, arguing that the authority provided to intelligence agencies under the 2008 FISA amendments is too broad and allows for the illegal searching of U.S. citizen's private communications, such as *ACLU v. Clapper* (2015) and *Wikimedia v. NSA* (2016). On November 17, 2016, the ACLU filed a third lawsuit against the NSA, DOJ and CIA, alleging that the agencies are withholding important information from American citizens and refusing to respond to Freedom of Information Requests (*ACLU v. NSA*, 2016). The suit suggests that Section 702 of the FISA Amendments Act of 2008 provides federal intelligence agencies with the power to conduct warrantless surveillance on U.S. citizen's communications (*ACLU v. NSA*, 2016). Section 702 permits surveillance of people located outside of the United States. However, the ACLU argues that the communications of Americans who are in contact with foreigners could be accessed under the law (*ACLU v. NSA*, 2016). The purpose of the section is to collect foreign intelligence information in order to keep the United States safe from external threats. The ACLU alleges that the government uses the PRISM surveillance program to access online communications such as email and social media through

companies like Apple and Facebook (*ACLU v. NSA*, 2016). In addition, the organization claims that the government uses Upstream surveillance to intercept telephone calls that go through large communications companies such as AT&T and Verizon. Using these programs, the ACLU argues that the government is able to conduct bulk searches of international online communications (*ACLU v. NSA*, 2016). A particularly serious problem with Section 702 surveillance is that there is little judicial review and individual probable cause is not required (*ACLU v. NSA*, 2016). According to the lawsuit, in 2015 the government needed only one court order to gather communications related to 94,368 targets (*ACLU v. NSA*, 2016). The ACLU argues that the U.S. public simply does not have the information necessary to understand how Section 702 surveillance works and if the government is violating privacy rights (*ACLU v. NSA*, 2016). Those in the privacy and security field agree that the implications of Upstream surveillance and retention of data are confusing (Eoyang, 2016). Mieke Eoyang, a privacy and security researcher, offers a helpful explanation of Upstream surveillance. She indicates that when a message is sent via email, it is broken down into various fragments called "packets" (Eoyang, 2016, p. 4). These packets contain a mix of metadata, which is the information regarding the communication, and content, the actual text of the communication (Eoyang, 2016). The packets may then be sent all over the world before they arrive at their destination (Eoyang, 2016). For example, a message packet from Paris might be routed through serves in Virginia and Georgia before arriving in Stockholm and being reassembled on the recipient's device (Eoyang, 2016). Along the way, U.S. intelligence may be able to intercept the message when it is on U.S. soil. Eoyang (2016) states:

> For the U.S. intelligence community, the emergence of the global Internet was a double-edged sword. On the one hand, it became difficult to distinguish between domestic and International communications; parts of an e-mail exchange between two people living in Atlanta travel through Cairo. On the other hand, the distributed

> design of the Internet provided easy access to foreign intelligence once huge volumes of purely international communications began flowing through the United States (p. 4).

The Privacy and Civil Liberties Oversight Board (PCLOB), which is an independent, bipartisan agency within the Executive Branch that works to ensure that the government's national security efforts do not violate U.S. citizens' privacy and other civil rights, also has concerns about government surveillance and the violation of privacy. In a 2016 report, the PCLOB made it clear that Section 702 contains some cause of concern (Recommendations Assessment Report, 2016). For example, though Section 702 surveillance targets foreign individuals, the report states that the FBI, NSA and CIA are able to use Section 702 data to gather information about U.S. citizens (Recommendations Assessment Report, 2016). The PCLOB recommended that the agency should be able to provide clear facts as to why information involving a U.S. citizen is necessary and reasonably likely to help in efforts to collect foreign intelligence (Recommendations Assessment Report, 2016). The report suggests that federal agencies are working to implement its recommendations but have not yet finished (Recommendations Assessment Report, 2016). The report further suggests that the NSA's Upstream collection technique does collect domestic communications and that the amount of those communications could be substantial. (Recommendations Assessment Report, 2016). The PCLOB recommended that the government work to find technology that can better stop the acquisition of domestic communications (Recommendations Assessment Report, 2016). Though the government has agreed to periodically assess its technology to ensure it is the best option available, it has determined that nothing better is currently available (Recommendations Assessment Report, 2016). The PCLOB is also concerned with "about" collection. "About" communications are messages that are not from or to the government's target but rather about

him or her (Recommendations Assessment Report, 2016). These are communications between non-targets, which the PCLOB believes can lead to privacy violations (Recommendations Assessment Report, 2016). The PCLOB suggests that "about" collection "present[s] novel and difficult issues regarding the balance between privacy and national security" (Recommendations Assessment Report, 2016, p. 22). It recommended that the NSA develop technology that would ensure the agency does not gather unnecessary information regarding non-targets (Recommendations Assessment Report, 2016). The NSA has indicated that it currently uses the best technology available but will periodically conduct studies to find out if better technology exists (Recommendations Assessment Report, 2016).

Although civil rights groups show concern over surveillance and privacy issues, it is less apparent whether individuals feel the same way. A 2015 Pew research study suggests that people are willing to give up privacy for convenience (Rainie & Duggan, 2016; LaFrance, 2016). Many of the 416 U.S. adults who took part in the study said they were willing to allow stores to track them in order to access bargains through loyalty cards (Rainie & Duggan, 2016.) Even more people said they were willing to allow their doctor to upload their medical history and records to a website, so that they could have the benefit of being able to access their records as well (Rainie & Duggan, 2016). However, the study also indicated that people were often resentful about what happens to their information once they share it (Rainie & Duggan, 2016). A previous Pew study also suggested that, though people in the United States complain about the erosion of privacy, they are willing to take only small steps to protect their online data, and some of the respondents seemed simply resigned to the idea that privacy is coming to an end (LaFrance, 2016). It appears that although people say they are concerned about privacy, they are also willing to give it up in exchange for a benefit.

*Privacy vs. Data Security*

When examining the evolution of privacy in the digital age, it is important to evaluate the boundaries of privacy. Specifically, one must consider where the security of data fits into the puzzle. Brandeis and Warren realized long before the advent of the Internet that technology could soon become a tool used to invade the rights of others (Warren & Brandeis, 1960). Over time, the right to privacy has become such a broad topic that scholars have debated and proposed various definitions to describe the true meaning of the word (Gormley, 1992). Many scholars agree that the concept of privacy must evolve along with technology (Florek, 2013). Some have used the terms "data security" and "information privacy" interchangeably, often arguing that privacy and information security are one and the same (Kasdan, 2011; Mills, 2008; and Schwartz, 2013). Still others argue that data security and information privacy are distinct concepts with distinguishable objectives requiring separate statutory attention (Henry, 2015; Bambauer, 2013). Some scholars on the latter side of the argument suggest that privacy focuses on an individual's decisions regarding who should receive permission to access personal information, while data security, on the other hand, involves technological measures used to regulate the access to private information (Bambauer, 2013).

Privacy and data security should be treated as distinct issues. If an individual decides to share personal information with a company and the company then shares that information without the individual's permission there would be a breach of privacy (Bambauer, 2013). A data security breach, on the other hand, would take place if the company unwittingly allowed a third party access to the information through cyber theft (Bambauer, 2013). Some have further suggested that a breach of privacy (*e.g.* a company's purposeful release of an individual's private information) harms the individual while benefiting the company (Bambauer, 2013). On the other hand, a breach of data security is harmful to both the individual and the company (Bambauer,

2013). Privacy violations, with some limited exceptions, tend to involve the publication of personal information without permission. However, data breach cases are about the failure to adequately protect data. Moreover, privacy violations would require the company to take some sort of action in furtherance of the breach. For example, intrusion upon an individual's solitude requires the act of intrusion and the publication of embarrassing facts requires the act of publication. Data security is about a company's omission or nonfeasance that subsequently leads to the loss of information.

The harm in privacy cases is also different than that of a data security breach. The injury in a privacy case includes harm to the victim's feelings (Warren & Brandeis, 1908) and reputation (Prosser, 1960) through the publication of personal information. Thus, it is the act of publishing the private information or intruding on solitude (Prosser, 1960) and the subsequent mental distress and suffering that are at the foundation of the right of privacy (*Cantrell*, 1974; Prosser, 1960). The harm in a data breach case is more akin to a breach of fiduciary duty (Solove, 2008). In other words, the injury that a victim experiences in a data breach case is not the emotional harm that comes from the publication of private information. Rather, it is the breach itself (*i.e.* the loss of information by the company) that is the harm (Solove, 2008). As Daniel Solove (2008) indicated in his article regarding privacy on the Internet, "The virtue of the breach of fiduciary duty approach is that this tort understands the breach to be the harm" (p. 122). Indeed, some scholars have suggested that companies that collect personal data should be held to a fiduciary duty standard (Litman, 2000) because the release of the information without permission would be a breach of confidentiality (Solve, 2008; Bambauer, 2013). This argument has been made primarily in the context of the *purposeful* release of private information, which would be an invasion of privacy issue (Litman, 2000). However, a similar argument could also

be made in data breach cases where there is a *theft* of information rather than a purposeful release. While duty of confidentiality may work for breach of privacy cases, the duty of care would be more appropriate for data breach cases. In fact, Solove (2008) suggests that the 'breach of fiduciary duty approach" (p. 123) could be used in data breach cases.

**Part 2: Conceptualization of privacy and its relationship to government surveillance**

This study examines various conceptualizations of privacy, but does not attempt to manufacture an all-encompassing definition of the word. Rather, this review of privacy research provides an avenue to operationalize the understanding of the word for this specific study and link privacy and surveillance.

As a result of Warren and Brandeis's law review article, multiple privacy rights were formed. The courts have interpreted privacy rights in the language contained in the First Amendment, Fourth Amendment, Ninth Amendment and Fourteenth Amendment, along with tort law and the rights contained in statutory law and state constitutions (Gormley, 1992). At its very basic foundation, Black's Law Dictionary defines the word private as confidential information that belongs to a person "as opposed to the public or the government" (Garner, 2006, p. 563). Privacy law is defined as a "statute that protects a person's right to be left alone or that restricts public access to personal information" (Garner, 2006, p. 563). Various scholars have attempted to define privacy, and though it may seem easy, as will be illustrated below, it is not.

Scholars suggest that the conceptualization of privacy goes much deeper than the definition provided in Black's Law Dictionary. For example, privacy involves the right to control personal information (Gormley, 1992), interpersonal boundaries (Altman, 1976), and one's body, thoughts and reputation (Solove, 2002). It also involves "freedom from surveillance" and "protection from searches and interrogations" (Solove, 2002, p. 2). Solove (2008) says the

concept of privacy is so sweeping and in such disarray that no one can truly define what it means. Indeed, as a concept, privacy can be viewed and examined multiple ways. For example, it can be looked at from the angle of what types of practices people consider to be private (Solove, 2000), or it can be analyzed by the kinds of acts that invade the practices of others (Solove, 2006). Solove (2006) proposes that there are four groups of acts that can harm privacy: "(1) information collection, (2) information processing, (3) information dissemination, and (4) invasion" (p. 488). In addition, scholars have studied privacy both through its legal aspects and as an analysis of human behavior (Solove, 2006; Acquisti, Brandimarte, & Loewenstein, 2015).

Research regarding privacy and human behavior suggests that people may not truly understand what privacy means or the consequences related to publishing private information (Acquisti, Brandimarte, & Loewenstein, 2015). Additionally, research suggests that people's concerns about privacy may be manipulated by others, such as commercial businesses and the government (Acquisti et al., 2015). Behavioral economic research indicates that people take many things into consideration when determining privacy boundaries such as the cost and effectiveness of their action (Acquisti, & Grossklags, 2005). People may also underestimate the risk of releasing private information or be influenced through psychological distortion, which include problems with self-control and the need for immediate gratification (Acquisti, 2004).

Contextual integrity, a term and framework coined by Helen Nissenbaum (2004), examines privacy by looking at how and why information flows from one person to the next or from a person to another entity (Barth, Datta, Mitchell, & Nissenbaum, 2006). Contextual integrity research proposes that decisions about privacy are based on the context and the specific information being shared (Barth et al., 2006). The framework assumes that all functions of life involve some sort of information flow (Nissenbaum, 2004). Moreover, there are certain norms

regarding information flow that must be upheld (Nissenbaum, 2004). When those norms are upheld, contextual integrity is maintained; however, a violation of those norms means a violation of contextual integrity (Nissenbaum, 2004).

Sandra Petronio (2002), who proposed the communication privacy management (CPM) theory, suggests that people put boundaries around information that they want to be considered private. The CPM theory, which is a dominate theory of privacy, is based on the idea that individuals believe they have ownership of their personal information and that they have the right to control who has access to that information (Petronio, 2002). People then use boundaries, which can be controlled and regulated, to separate private information from their public relationships (Petronio, 2002). According to the theory, individuals think they should have control over their private information even after they grant access to the information to others (Petronio, 2013). CPM "offers a privacy management system that identifies ways privacy boundaries are coordinated between and among individuals" (Petronio, 2002, p. 3). Using an example of a small group of friends, the theory indicates that one individual in the group could decide to share private information with another person in the group (Petronio, 2013). Thus, the first individual, or owner of the information, grants access to a co-owner (Petronio, 2013). The owner could even grant access to multiple co-owners (Petronio, 2013). Then the owner would negotiate boundaries with the co-owners to determine whether the information can be shared with third-parties (Petronio, 2013). When formulating the foundation for the CPM theory, Petronio (2002) proposed five basic beliefs: 1) private information; 2) boundaries that separate private information and public relationships; 3) control; 4) a rule-based management system to aid in boundary regulation; and 5) privacy and disclosure are treated as dialectic. Petronio (2002) believes that these "[f]ive fundamental suppositions define the nature of CPM" (p. 3). Over time, the theory

has evolved. In a CPM status report Petronio (2013) indicated that the theory has become more streamlined over time. There are now three main elements that "represent the system of [CPM]" (p. 8): 1) Privacy ownership; 2) privacy control; and 3) privacy turbulence.

What this review of privacy research illustrates is that pinning the term down with a precise definition or theory is likely not possible. Instead, a better option may be to define privacy based on what type of issue or problem one is examining (Solove, 2002). In the present study, the issue being analyzed is surveillance, and as will be explained next, surveillance is a type of privacy violation. Solove (2002) proposed that violations of privacy involve a disruption of a person's actions, traditions and decisions, such as communicating with others. According to Solove (2002), surveillance, which is a way to collect information (Solove, 2006), is a type of disruption. Solove (2002) suggested that "Being watched can destroy a person's peace of mind, increase her self-consciousness and uneasiness to a debilitating degree, and can inhibit her daily activities. We may want to protect against surveillance not merely to prevent disruptions of certain practices but to foster practices or to structure society in a particular way (by restricting the power of the government or employers)" (p. 22). Moreover, surveillance can be used as a tool to control people's behavior (Solove, 2006). In its appeal of the district court's decision in *Wikimedia v. NSA* (2015), the ACLU argued that the governmental surveillance allowed under PRISM violated the privacy rights of Americans who communicate internationally (*Wikimedia v. NSA*, 2016). They likened the surveillance to the government opening Americans' mail and reading the contents in search of illegal activity (*Wikimedia v. NSA*, 2016). The attorneys suggested that privacy includes the ability to conduct communications without the concern of warrantless governmental intrusion (*Wikimedia v. NSA*, 2016). Thus, at its very foundation, surveillance is about privacy. The two concepts are interrelated in such a way that when

considering issues of governmental surveillance in the United States, one must include an examination of privacy interests and expectations.

Solove (2002) proposes that scholars should not attempt to conceptualize privacy by trying to define it as "an abstract conception" (p. 21); instead, understanding privacy begins by identifying "specific contextual situations" (p. 21). Rather than attempting to define all that privacy is, this study conceptualizes it as "freedom from surveillance." Thus, consent to allow the surveillance of personal communications would be a decision to give up a degree of privacy.

When talking about privacy, and when people are willing to give it up, it is important to also note the "privacy paradox." The "privacy paradox refers to a discrepancy between an individual's attitude toward privacy and her behavior regarding privacy" (Acquisti, Brandimarte & Loewenstein, 2015). In other words, people will say they have significant privacy concerns regarding their personal information, yet they will share that information with a retail company in order to receive the benefits of a loyalty card (Acquisti, Brandimarte & Loewenstein, 2015). Studies of privacy and behavior economics may provide an answer to the paradox.

Acquisti (2004; Acquisti & Grossklags, 2005) indicates that people may not be able to make rational decisions about privacy because of psychological distortions and an inability to gather, and comprehend, all of the information necessary to make an informed decision. For example, when deciding to share private information, an individual may not have the full information about the related risks and technology that can keep information secure (Acquisti, 2004; Acquisti & Grossklags, 2005). Even if the individual did have all of the requisite information, she may be limited by "bounded rationality" (Acquisti, 2004, p. 23; Acquisti & Grossklags, 2005). Bounded rationality "refers to the inability to calculate and compare the magnitudes of payoffs associated with various strategies the individual may choose in privacy-

sensitive situations" (Acquisti, 2004, p. 23; Acquisti & Grossklags, 2005). Another issue could be related to psychological distortions, such as hyperbolic discounting, which "implies inconsistency of personal preferences over time – future events may be discounted at different discount rates than near-term events (Acquisti, 2004). Hyperbolic discounting could lead to taking few precautions in the present to ensure security in the future (Acquisit, 2004).

Acquisti (2004) suggests that immediate gratification, which is related to hyperbolic discounting, could explain the privacy paradox. Acquisti (2004) uses the words of O'Donoghue and Rabin (2001, p.4) to explain immediate gratification. Basically, the term means that "A person's relative preference for well-being at an earlier date over a later date gets stronger as the earlier date gets closer…People have self-control problems caused by a tendency to pursue immediate gratification in a way that their 'long-run selves' do not appreciate" (Acquisti, 2004, p. 24). The example Acquisti (2004) offers is quite simple. If, on Monday, a person was given two options, she could either 1) work for 5 hours on Saturday or 2) 5 and a half hours on Sunday, she would likely choose to work 5 hours on Saturday. However, if asked again on Friday, she will be more likely to change her answer and decide to work 5 and half hours on Sunday (Acquisti, 2004). As the time for her to work got closer, she was more likely to want to placate her current self at the expense of her future self. When placed in the context of privacy, this could mean that a person is more willing to share private information with others if there is a current benefit, while not fully considering the risks or harm that could come to him in the future. Acquisti (2004) further states that "when costs are immediate, time-inconsistent individuals tend to procrastinate; when benefits are immediate, they tend to preoperate" (p. 26). Thus, if the benefit of sharing private information comes before the cost/risk, it is likely individuals will discount the future risk. This seems to help explain the privacy paradox. In

addition, benefits do not have to be monetary or tangible. Some research suggests that the use of social media, like Facebook, can create social capital, which is related with positive effects to society such as increased health and lower crime rates (Ellison, Steinfeild & Lampe, 2007). If social capital is a benefit that an individual knowingly or subconsciously seeks, this could explain why people are willing to share intimate details on social media even while they tout the importance of privacy.

Whether the issue of the privacy paradox stems from an inability to process privacy risks or a time inconsistency that leads to immediate gratification and harm to the future self, there is evidence that a privacy paradox exists. This is important because some scholars suggest that an explanation for the paradox is so elusive because the paradox itself is illusory (Acquisti et al., 2015). These scholars propose that attitudes, intentions and behaviors toward privacy should not be expected to be related, so it is not paradoxical for a person with a high privacy concern to share personal information (Acquisti et al., 2015). In other words, a person may believe that privacy is important but that belief has no relationship with the person's intention to share personal information with a department store in exchange for benefits. However, Acquisti et al. (2015) were not satisfied with that explanation because some studies have provided empirical evidence that privacy attitudes, behaviors and intentions are related. Thus, there is evidence that the privacy paradox is a supportable theory, and this current study examined whether the privacy paradox exists when increased government surveillance of online activity is involved.

## Chapter 3: Theoretical Foundation

This section discusses the theoretical foundation for the study. This study relies on Extended Parallel Process Model (EPPM) in order to investigate the relationship between fear

and privacy. In addition, this study extends EPPM research by determining if there is a relationship between cognitive dissonance and the rejection of a message that promotes governmental access to private communications.

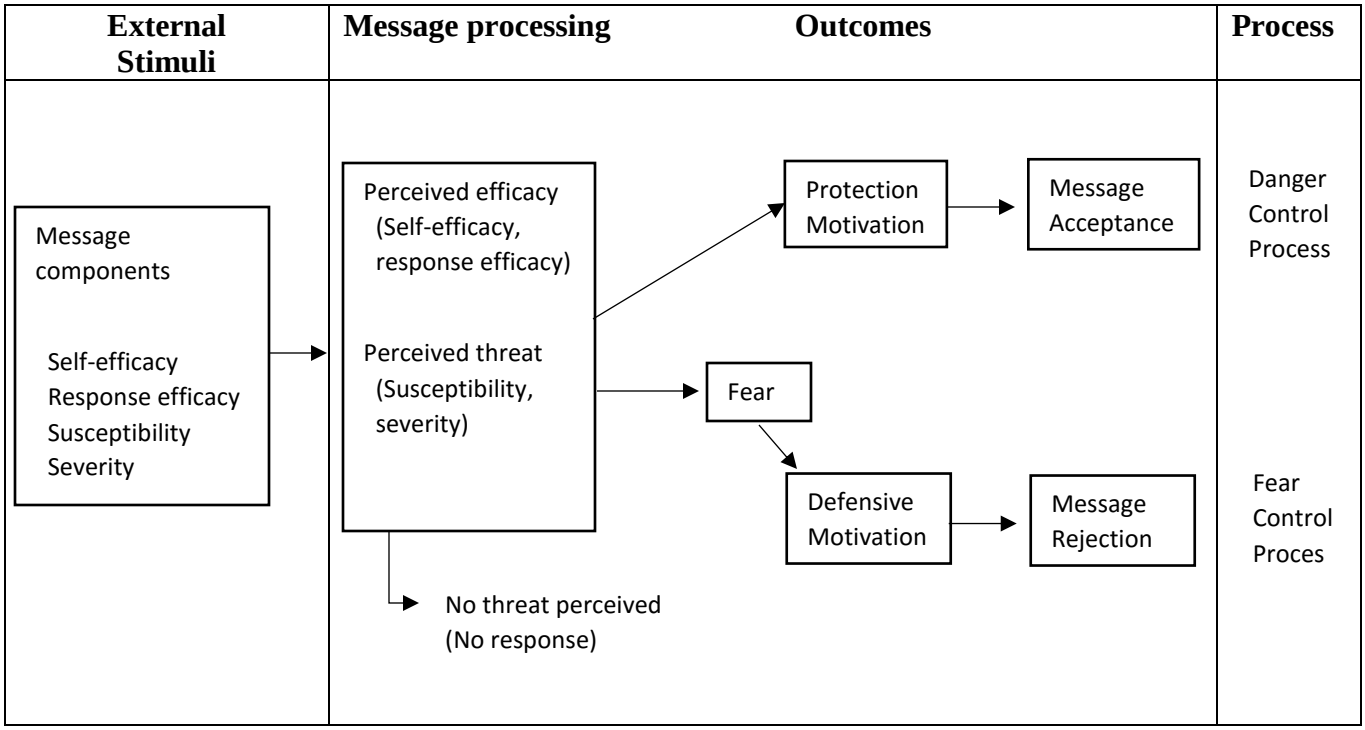
**Extended Parallel Process Model**

As illustrated in the Literature Review, there is a clear link between privacy and government surveillance both legally and theoretically. This study focuses on the conceptualization of privacy that highlights freedom from surveillance, and under the Fourth Amendment to the U.S. Constitution, U.S. citizens have a right to privacy that prohibits unreasonable governmental intrusion. As noted previously, courts have applied that right of privacy to various types of communication including phones, computers, and social media. Thus, under current law, the government cannot arbitrarily use surveillance to monitor the communications of U.S. citizens. There is also a clear link between government surveillance and national security, which was the reason the U.S. government began the PRISM project. The main purpose of the program was to monitor for possible terrorist activity. The government argued that by intercepting terrorist communication, it could stop threats against the United States and its citizens. Privacy advocates argued that the PRISM program had the possibility of allowing the government to monitor the communications of U.S. citizens without first obtaining a warrant; thus, allowing for a breach of privacy. It is logical, however, to ask whether some individuals may be willing to give up their constitutional right to privacy if it means keeping them safe from the threat of terrorism. When considering the privacy paradox, it is logical that some will willingly trade privacy for security, even if they have a high regard for privacy. Moreover, the decision to give up privacy to increase security could stem from fear. Because EPPM examines the effects of fear appeals, it is an appropriate theory to test the extent to which people are

willing to waive their privacy rights because they are scared of terrorism. This section provides a thorough explanation of EPPM's assumptions and processes.

Researchers suggest that fear appeals can result in a cognitive process that drives an individual to make attitude and behavioral changes based on the effects of the appeal (Witte, 1994; Maloney, Lapinski, & Witte, 2011). EPPM explains why fear appeals have persuasive effects. The underlining assumption of the theory is that if a person feels fear, that person will take some sort of action to alleviate the fear (Gass & Seiter, 2007). Furthermore, it assumes that people process fear appeals both cognitively and emotionally (Witte, 1994). EPPM proposes that when a person receives a message that contains a fear appeal, that person will begin to appraise the message using two routes: danger control process and fear control process. Depending on which route is dominant, the person has three possible options: no response, danger control or fear control (Witte, 1994; Maloney, Lapinski, & Witte, 2011). The process may then lead to acceptance or rejection of the persuasive message (Witte, 1994). This theory, proposed by Kim Witte (1994), melds together Leventhal's parallel process model, which proposed the two processing routes (i.e. fear control and danger control) and Roger's protection motivation theory, which focused on the danger control process (Witte, 1994). Fear "has been conceptualized as a motivational state protecting one against danger" (Rogers, 1983, p. 155). Rogers (1983) indicated that fear mediates attitude change. A fear appeal is operationalized as communication that sets forth a threat that is then followed "with a recommended response to avert the threat" (Witte, 1993, p. 147).

**Figure 1.** The extended parallel process model (Maloney et al., 2011)




In order to persuade the audience, the message attempts to elicit fear by illustrating a threat, which could be portrayed by a danger that is relevant to the person in some way (Witte, 1994; Maloney, Lapinski, & Witte, 2011). The threat within the fear appeal contains two elements: perceived severity and perceived susceptibility (Witte, 1994; Maloney, Lapinski, & Witte, 2011). Perceived severity refers to the significance of the danger or threat, and perceived susceptibility is related to whether the person thinks the threat represents an actual risk to him or her (Witte, 1994; Maloney, Lapinski, & Witte, 2011). The manipulation of the level of the threat has been found to have an effect on the amount of fear people feel (Rogers, 1983).

The recommended response contained in the fear appeal, or efficacy, offers a route for people to combat or overcome the threat through efficacy (Witte, 1993). Witte (1994) indicates that efficacy has the ability to counteract fear. Thus, if the message recommends a response or action in order to protect oneself from the threat, the person will evaluate that action using

efficacy (Witte 1994). EPPM incorporates an examination of two kinds of efficacy: perceived response efficacy and perceived self-efficacy (Witte, 1993; Witte, 1994; Maloney, Lapinski, & Witte, 2011). Response efficacy examines how the person perceives the likelihood of the action's success, and self-efficacy refers to whether the person believes he or she is able to conduct the recommended action (Witte, 1994).

EPPM proposes that once a person receives a message that contains a fear appeal two appraisal processes will be initiated (Witte, 1994). First, the person will consider the degree of threat (Witte, 1994). If there is no threat or if the threat is very minor, the person will not be motivated to begin the second appraisal process (Witte, 1994; Maloney, Lapinski, & Witte, 2011). In that case, the person may take no response to the threat. However, if the perceived danger of the threat is high, then the person is more likely to start the second process: The efficacy assessment, where the person will consider whether the recommended action will fix the threat and if the person can successful conduct the action (Witte, 1994).

If the message the person encounters does contain a significant threat, EPPM suggests that the individual will have one of two possible reactions (Witte, 1997). The first is to become scared and have an inability to act, which leads to defensive behaviors such as denying that a threat exists (Witte, 1997). This reaction is called fear control. The second possible reaction is to become motivated to understand the risk and work toward a solution or way to reduce the threat (Witte, 1997). This reaction is called danger control. Thus, EPPM suggests that fear appeals lead to two possible outcomes: danger control or fear control (Witte, 1997). The levels of perceived efficacy have an effect on which process the individual will choose. (Witte, 1997).

According to EPPM, the danger control process will be initiated and the person will accept the message's recommendation and make changes to her attitude if the person perceives a

high level of threat and has high efficacy (Witte, 1994; Maloney, Lapinski, & Witte, 2011). For example, Witte et al. (1998) found that participants who were exposed to a fear appeal message that conveyed a high threat of genital warts transmitted through sexual intercourse and then offered condom use as the high efficacy recommendation were more likely to have positive attitudes toward condom used as compared to those exposed to a low efficacy recommendation. According to Witte (1994) the danger control process, which is cognitive in nature, has four components. First, the person perceives the threat and understands she is at risk. Second, the person feels a high level of efficacy because she thinks she can take action to alleviate the risk. Third, once that high level of efficacy is established, the person feels motivated to protect herself. Finally, the person "deliberately and cognitively confronts the danger" (Witte, 1994, p. 115). This leads to an acceptance of the recommended response contained within the message (Witte, 1997). This last stage, message acceptance, is where the person's attitude may change in order to alleviate the threat (Witte, 1997). When using the danger control process, people become motivated to protect themselves (Witte, 1997). They recognize the threat and believe that they can take action to prevent or overcome it (Witte 1997).

Witte (1994) further explains, however, that if a person perceives a high threat and has low efficacy, then fear control process is initiated and the person will be on the defensive and will likely reject the message recommendation (Witte, 1994). For example, Witte et al. (1998) found that participants who were exposed to a message that conveyed a high threat of genital warts and low efficacy of condom protection were less likely to have positive attitudes toward condom use than those who were exposed to high efficacy. Witte (1994) explains that while danger controls are cognitive in nature, fear controls tend to be part of an emotional response. Danger controls lead the person to think about the threat and consider action to combat it, while

fear controls are focused on how to handle the terror and stress the person feels in regard to the threat (Witte, 1994). In order to control their fear, people will navigate toward defense motivation, which means they will push the threat from their minds or will convince themselves that the threat is not significant (Witte, 1994). This process leads to rejection of the message's recommendation (Witte, 1994).

The degree of threat controls the strength of the person's rejection or acceptance of the message recommendation, while the amount of efficacy controls whether the person decides to use fear control or danger control (Witte, 1994). If the threat level is low, however, EPPM suggests that there will be no relationship between efficacy level and message acceptance or rejection (Witte, 1994). Thus, there are basically three possible outcomes to a fear appeal. First, if a person does not perceive any sort of threat then there will be no response to the message at all because the motivation to fully process the message and respond has not been initiated (Roberto & Goodall, 2009). Second, if the person perceives a serious threat and has no way to combat the threat (*i.e* little or no efficacy) that person will gravitate toward the fear control process (Roberto & Goodall, 2009). Finally, if the person perceives a high threat and believes that he or she can act to alleviate the threat (perceived high efficacy) that individual will choose the danger control process (Roberto & Goodall, 2009). According to EPPM scholars, if a company, such as a health organization, wants to persuade people to make better lifestyle choices, it will use messages that contain a fear appeal with high efficacy in order to steer people toward the danger control process, which includes accepting the message's recommendation and making attitude and behavioral changes (McMahan, Witte, & Meyer, 2009; Smith, Rosenman, Kotowski, Glazer, McFeters, Keesecker, & Law, 2008).

Witte, Berkowitz, Cameron and McKeon (1998) indicate that EPPM is a "health risk message theory" (p. 572), and much of the previous research using the theory has focused on health communications. Using EPPM, Witte has investigated the effectiveness of health campaigns (Witte & Allen, 2000). Specifically, she has used the theory to examine messages about teenage pregnancy (Witte, 1997), preventing the spread of AIDS (Witte, 1994) and genital warts (Witte, Berkowitz, Cameron & McKeon, 1998), as well as the health risks of exposure to electromagnetic fields (McMahan, Witte, & Meyer, 2009). Similarly, other recent EPPM research has primarily analyzed health communications including messages regarding: kidney disease (Roberto & Goodall, 2009); substance abuse (Choi, Krieger, & Hecht, 2013); bed bugs (Goodall & Reed, 2013); hearing loss (Smith et al., 2008); meningitis (Gore & Bracken, 2005); healthy eating (Napper, Harris, & Klein, W. M. (2014); melanoma (Shi & Smith, 2016); HPV (Carcioppolo, Jensen, Wilson, Collins, Carrion, & Linnemeier, 2013); and general health news (Hong, 2011). Moreover, EPPM has generally been used by scholars to analyze messages that are intended to persuade.

Although EPPM research is primarily health-related, it is logical that the theory can explain attitude changes due to non-health threats. In this study, it will be used to explain attitude changes regarding the right to privacy when a person is faced with the threat of terrorism. Moreover, the fear appeal used in this study will be formatted to read like a news article. Recent research suggests that the theory can be used to study news articles, which are not expressly meant to persuade but have an incidental persuasive or influential effect (Goodall & Reed, 2013; Hong, 2011). These types of messages, though non-persuasive in nature, have the ability to illicit fear. Hyehyun Hong (2011) conducted a study using EPPM to examine how audiences process the information conveyed in television news stories about health threats. In the study, Hong

(2011) assumed that health stories broadcast by TV news contain fear appeals because they present health risks and then offer recommendations to avert the risks. Hong (2011) discovered that some of the EPPM variables (perceived threat severity, response efficacy and self-efficacy) mediated the amount of influence health consciousness had on message acceptance. Goodall and Reed (2013) extended EPPM research by investigating news coverage regarding bed bugs. One focus of the study was to test the use of EPPM in messages that were non-persuasive (2013). Similar to Hong, Goodall and Reed (2013) suggested that health news stories likely contain fear appeals because they provide information about a health threat and then offer recommendation in living a healthy lifestyle. The Goodall and Reed (2013) study had an additional importance in that it researched an uncertain threat. Goodall and Reed (2013) suggested that the public was uncertain about the threat of bed bugs and how to stop them from spreading. Yet, the researchers also found that the public had fear regarding infestations (Goodall & Reed, 2013). The study asked whether uncertainty about the threat and efficacy have an effect on whether individuals sought more information about bed begs or practiced message avoidance. The results indicated that uncertainty as to a threat tended to cause people to seek out more information about bed bugs, while uncertainty about efficacy resulted in issue avoidance (Goodall & Reed, 2013).

This current study extends previous EPPM research. Studies using EPPM tend to test the theory on a variety of health topics, which focus on threats to an individual's wellbeing from a variety of conditions, ailments and infectious diseases. This study investigates to what extent EPPM's assumptions hold true in the context of the threat of terrorism. In this case, the fear appeal will be the danger of terrorist activity and the efficacy (*i.e.* the message containing the recommendation for action) will be the willingness to allow increased government surveillance. In other words, if people accept the efficacy recommendation and agree that increased

governmental monitoring of communications should be used to combat terrorism, they are also consenting to waive their right to privacy. As noted previously, breach of privacy is about the disruption of a person's actions, such as communication, and surveillance is one such type of disruption (Solove, 2002). Under the Fourth Amendment, the government cannot arbitrarily monitor the communications of all U.S. citizens. However, people have the ability to waive their privacy rights. This study investigates whether people will waive those rights when they are scared. Thus, the following hypotheses will be tested:

H1a: Those exposed to the high threat/high efficacy government surveillance fear appeal will have a higher message acceptance rate than those exposed to the high threat/low efficacy government surveillance fear appeal.

H1b: Those exposed to the high threat/high efficacy individual reporting fear appeal will have a higher message acceptance rate than those exposed to the high threat/low efficacy individual reporting fear appeal.

Message acceptance is more likely to occur when the person is exposed to a high threat/high efficacy recommendation (Witte, 1994; Witte et al., 1998). Thus, participants who are exposed to a high threat of terrorism and a high efficacy option of either increased government surveillance or individual reporting will be more likely to accept those efficacy messages. In other words, this suggests that individuals who are exposed to the high threat and high government surveillance efficacy option will be more willing to waive their privacy rights by consenting to increased surveillance.

This study also investigates whether the relationship between level of efficacy and message acceptance remains depending on the type of high efficacy offered. This study tests two efficacy options: 1) increased governmental surveillance and 2) relying on individual reporting

of suspicious activity to law enforcement. The aftermath of the PRISM scandal has made it clear that the right to privacy is important to many people in the United States. Indeed, the ACLU filed a lawsuit against the NSA arguing that the type of surveillance used by the PRISM program violated Americans' privacy rights (*Wikimedia v. NSA*, 2016). Moreover, the right of privacy came up again more recently when the FBI attempted to gain access to the iPhone used by one of the San Bernardino attackers (Benner & Lichtblau, 2016; Selyukh & Domonoske, 2016). There is no question that the courts have inferred a right to privacy within the Fourth Amendment because it is a critical part of the country's foundation. Thus, it is possible that people will be more willing to accept an efficacy recommendation that involves individual reporting than one that calls for increased government monitoring of communications. This study will test the following:

RQ1: Is there a significant difference between the message acceptance rate of those who were exposed to the government surveillance efficacy option as compared to those exposed to the individual reporting efficacy option?

H2a: Those exposed to the government surveillance high threat/high efficacy option will have more favorable attitudes toward government surveillance than those who were not.

H2b: Of participants who have a greater level of privacy concern, those who are exposed to the increased surveillance high efficacy option will have more favorable attitudes toward government surveillance than those who are exposed to the other efficacy options.

H2c: There will be a positive relationship between the perceived threat of terrorism and attitudes toward government surveillance.

EPPM tests whether a fear appeal can persuade an individual to accept a recommendation for action (Witte, 1994). In this case, those who are exposed to the government surveillance high efficacy recommendation will likely be persuaded by the fear appeal to accept that recommendation. However, those who are exposed to a different efficacy option will not have the opportunity to be persuaded by that particular message and will likely have more negative opinions about government surveillance. These questions are important because they not only examine the extent to which people will accept government surveillance as compared to individual report, they also investigate a concept that has not yet been studied by researchers. Scholars using EPPM have examined why efficacy has an effect on persuasion (Witte, 1994), threat-to-efficacy ratios (Carcioppolo et al., 2013), and how different types of efficacy are related (Choi, Krieger, & Hecht, 2013). However, none of the studies have investigated how opinions regarding efficacy can affect persuasion. For example, Witte (1994) indicates that if a person perceives a threat and believes that she has efficacy to combat the risk, she will navigate toward the danger control process and message acceptance. However, would the result be the same if the person is provided with a high, yet undesirable, efficacy option? For example, if a person considers terrorism as a threat and believes that increased government surveillance is a viable option, will the individual be less likely to accept that option if he or she has a higher concern for privacy? As noted previously, studies indicate that U.S. citizens tend to value privacy, though they will give it up for certain benefits. This study uses EPPM in order to discover whether fear appeals regarding terrorism could persuade individuals to have favorable attitudes toward increased government surveillance.

This study also considers the privacy paradox. Thus, this study also tests the following:

RQ2: Is there a negative association between privacy concerns and attitudes toward government surveillance?

H3a: In the government surveillance groups, privacy and fear control will have a positive correlation.

H3b: In the individual reporting group, privacy and fear control will have a positive correlation.

Logic will tell us that there should be an association between privacy and attitudes toward government surveillance. If studies show that people in the United States covet privacy and governmental surveillance is an invasion of privacy, then people with high privacy rates should have more negative attitudes toward government surveillance. This should also mean that as the need for privacy increases, the rejection of the government surveillance message should also increase. However, the privacy paradox suggests the opposite is true. Even though people want privacy, they will willingly give it up for a benefit (Acquisti, Brandimarte & Loewenstein, 2015). In this case, the benefit is safety from terrorism, both nationally and individually.

**Cognitive Dissonance**

This study extends EPPM research by examining if there is a relationship between cognitive dissonance, message rejection and message acceptance. In addition, this study also advances privacy research by investigating to what extent dissonance is associated with privacy concerns. This section provides a review of cognitive dissonance.

Cognitive dissonance refers to inconsistencies between an individual's beliefs and actions. The theory proposes that if an individual has an inconsistency in her beliefs and

behaviors it can lead to discomfort (Festinger, 1962). According to the theory, the individual will want to alleviate the discomfort and will do that by reducing the dissonance in order to "achieve consonance" (Festinger, 1962, p. 3). In other words, if an individual is dealing with an inconsistency between what she believes and how she acts, there must be some sort of change in order to bring her beliefs and actions back into harmony. Festinger (1962) uses the word "dissonance" to replace inconsistency and the word "consonance" to replace consistency. In addition to attempting to bring beliefs and actions back into harmony, the theory also proposes that individuals will avoid situations that could increase the inconsistency (Festinger, 1962). Festinger (1962) explains that cognitive dissonance is a motivating factor parallel to the feelings of hunger. If an individual is hungry, she looks for food (a way to alleviate the hunger). Cognitive dissonance is similar in that it causes an uncomfortable feeling that leads an individual to seek ways to alleviate the discomfort (Festinger, 1962; Kenworthy, Miller, Collins, Read & Earleywine, 2011). Moreover, research suggests that cognitive consistency is a primary motivational factor for people in general (Gawronski, 2012).

Once an individual is faced with an inconsistency, there are multiple avenues to reduce the dissonance. One way could be a change in behavior, and another way could be a change in knowledge or attitude toward a certain behavior, this could involve acquiring new knowledge (Festinger, 1962). Festinger (1962) used smoking as an example of cognitive dissonance. A smoker could believe that smoking is harmful for her health, yet she continues to smoke anyway (Festinger 1962). In that case, there is an inconsistency between that smoker's beliefs and her actions. The theory of cognitive dissonance suggests that the smoker will want to alleviate the discomfort of that inconsistency in some way. The smoker could attempt to reduce the dissonance by changing her actions – in other words, she can stop smoking (Festinger, 1962).

That would bring harmony back to her actions and beliefs. Another option would be to change her attitude by rationalizing her decision to keep smoking perhaps by convincing herself that the benefits of smoking outweigh the risk (Festinger, 1962; Kleinjan, van den Eijnden & Engels, 2009). For example, studies indicate that people who are able to justify smoking are less likely to quit the habit (Kleinjan et al., 2006). In other cases, dissonance can be persistent and may never truly end (Festinger, 1962). Even so, Festinger (1962) proposes that the individual will continue her efforts to reduce the dissonance.

This study extends cognitive dissonance research by examining whether dissonance is associated with the acceptance or rejection of a fear appeal recommendation. In particular, this study focuses on individuals' attitudes toward the efficacy options provided through the fear appeal. Cognitive dissonance suggests that when people are exposed to beliefs that are opposed to their own, an inconsistency will occur. Thus, it is likely that if a person has a positive attitude toward privacy and limited governmental intrusion, dissonance will result from a high efficacy option that involves increased governmental surveillance. Along the same vein, the person will likely feel less dissonance when faced with a high efficacy option that includes individual reporting of suspicious activity. What is unclear is how cognitive dissonance will affect the rates of message rejection and acceptance. The study by Hong (2011) found that an outside variable, health consciousness, was associated with threat severity, threat susceptibility, response efficacy and self-efficacy. Similarly, as illustrated in Figure 2, the current study examines to what extent cognitive dissonance affects threat and efficacy. Moreover, because the message involves consent to allow increased government surveillance, this study investigates in what way dissonance is associated with the decision to accept a message that promotes government monitoring of private communications.

**Figure 2: Relationship between cognitive dissonance and fear control (Hong, 2011)**

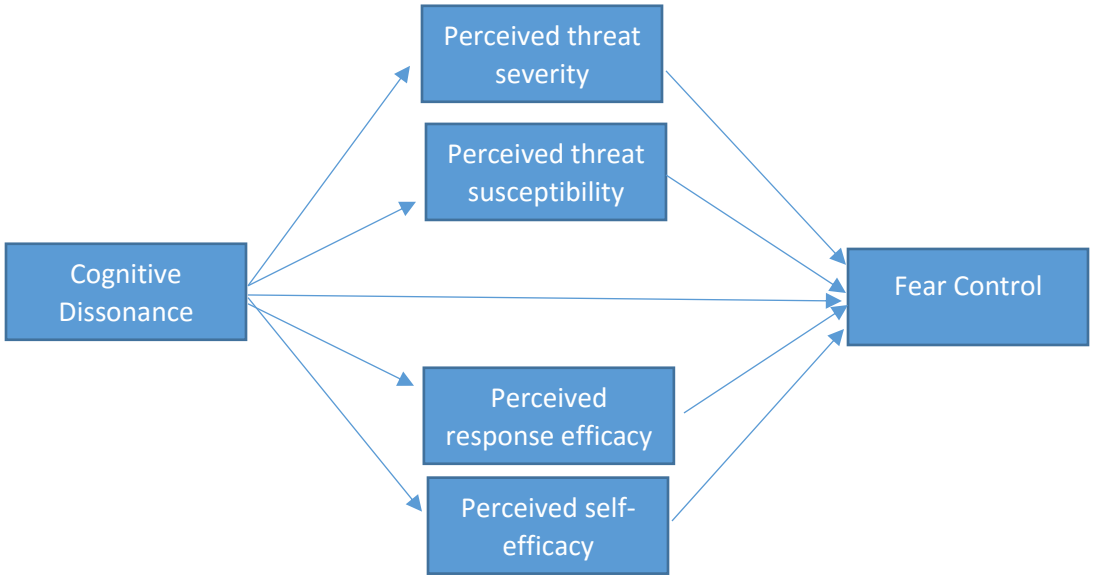
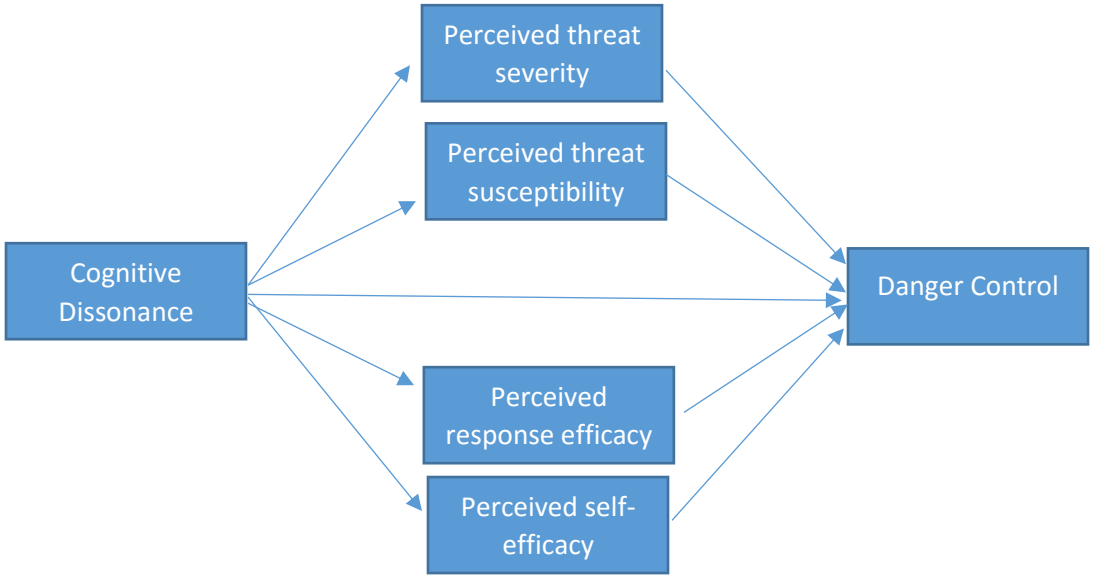



**Figure 3: Relationship between cognitive dissonance and danger control (Hong, 2011)**




Thus, this study investigates the following research questions:

RQ3a: Is there a significant relationship between level of dissonance and perceived threat severity?

RQ3b: Is there a significant relationship between level of dissonance and perceived threat susceptibility?

RQ3c: Is there a significant relationship between level of dissonance and fear?

Hong (2011) discovered that an outside variable, health consciousness, was positively associated with perceived severity of the threat. Similarly, it is likely that those who feel a greater dissonance when reading the threat will perceive a higher severity and susceptibility in the threat. Because fear leads to fear control and message rejection, it is also likely that dissonance could be associated to fear.

RQ4a: Is there a significant relationship between level of dissonance and response efficacy?

RQ4b: Is there a significant relationship between level of dissonance and self-efficacy?

Hong (2011) found that there was a positive relationship between health consciousness and both types of efficacy. According to Festinger (1962), dissonance causes a person discomfort, which he or she will want to alleviate through changes in action or attitude. In this case, if the participants feel uncomfortable about the threat of terrorism, it makes sense that they will want to use efficacy to alleviate the threat.

RQ5a: Is there a significant relationship between level of dissonance and fear control?

RQ5b: Is there a significant relationship between level of dissonance and danger control?

RQ5c: When controlling for fear, perceived threat and perceived efficacy, can cognitive dissonance predict a significant amount of variance in fear control?

RQ5d: When controlling for fear, perceived threat and perceived efficacy, can cognitive dissonance predict a significant amount of variance in danger control?

Hong (2011) also found that there was a direct relationship between health consciousness and message acceptance. It is likely that an outside variable like dissonance will also have an effect on message acceptance (danger control) and message rejection (fear control). In order to determine that relationship is not spurious, it is also important to test the association after controlling for the EPPM variables.

H5a: When isolating the participants in the government surveillance efficacy groups, privacy will have a positive association with dissonance.

H5b: When isolating participants in the government surveillance efficacy groups, there will be a negative relationship between the levels of dissonance and attitude toward government surveillance.

As noted previously, there is a link between privacy and government surveillance (Solove, 2002). In cases of the government using electronic devices to intercept communications, there are often questions surrounding privacy. Logically, those who highly covet privacy will be less likely to approve of government surveillance (though the privacy paradox calls that into question). Moreover, people feel dissonance when they are "forced to advocate for a position they disagree with" (Metzger et al., 2015, p. 13). Even viewing information that advocates for an ideology that the individual opposes can lead to dissonance (Metzger et al., 2015) Thus, those who are concerned about privacy will likely feel more dissonance when they read a message that advocates the use of increased government surveillance to combat terrorism. It is also likely that

those who are concerned about privacy will be less likely to approve of government surveillance as compared to those who are not as worried about privacy.

# Chapter 4: Method

The data for this study was collected using an online experiment to test EPPM on a non-health issue (terrorism) and examine the effects of cognitive dissonance on message acceptance. The experiment employed a 2 (severity of threat: high/low) x 4 (efficacy: low/high governmental surveillance; low/high individual reporting), along with a control group that received a generic message that had no relation to terrorism or government surveillance. There was a total of nine groups, with 40 people per group.

## Participants and procedure

The 360 participants were recruited using a Qualtrics panel. Qualtrics has a pool of more than a million people who have previously agreed to take part in a variety of surveys. These panelists join from a variety of sources such as airline customers who chose to join in a reward program for sky miles, retail customers who opt in to get points at a retail outlet or general consumers who participate for cash. Qualtrics randomly invited people from its current pool to participate in this experiment. The participants were rewarded based on their previous individual agreements with Qualtrics. Qualtrics determines the incentive based on each individual participant's profile data when they enroll to take part in Qualtrics surveys. Some people received monetary compensation, while others received rewards points or sky miles. The participants recruited for this experiment were U.S. citizens, 18 years or older. This study focuses on U.S. citizens for two reasons. The first is that the privacy rights (*i.e.*, freedom of governmental intrusion) emphasized in this study are based on the U.S. Constitution. Second, for the reasons laid out in the next section, fear appeals should be directed toward a certain audience. In this case, it makes sense to have the audience be people located within the United States. The

participants were instructed to access an online Qualtrics survey. The unit of analysis for this study is individuals.

Initially, each participant was sent an email from Qualtrics inviting them to take part in the experiment. Once they agreed to take part, they were automatically and randomly placed into one of the one of the eight experimental groups or the control group. In order to avoid priming the participants, a pre-test questionnaire was not conducted. Each participant read one article containing one of the manipulation pairs. For example, one group read an article that contained a high threat of terrorism and a high efficacy of increased government surveillance. A second group read an article that contain high threat of terrorism and a low efficacy of increased government surveillance, and so on. The control group read an article that was not related to terrorism or government surveillance. There was a total of nine articles. Each article was produced as if it was written and published by CNN. The articles were all of similar length with the longest being 489 words and the shortest being 466 words (see Figures 1 and 2). After reading the article, the participants were asked to answer a variety of questions pertaining to the variables explained later in this section.

**Figure 4.** Example stimulus

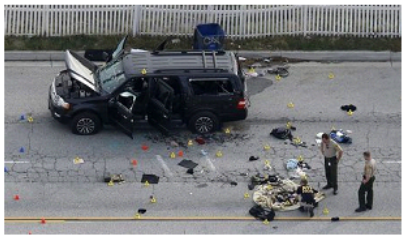
CNN

# Top U.S. intel official: ISIS can stage Europe-style attacks in U.S.

**By Christine Crowell, CNN**

**(CNN)** - ISIS has the capability to stage a Paris-style attack in the U.S. using local cells to strike in multiple locations and inflict dozens of casualties, according to the Obama administration's top U.S. intelligence official.

"That's something we worry about a lot in the United States," Director of National Intelligence James Clapper told CNN. "They could conjure up a raid like they did in Paris or Brussels," where March attacks on a train and at an airport left 32 dead and 300 people injured, Clapper said. The November 2015 Paris attacks killed at least 130.



*Law enforcement officers look over the evidence near the remains of the SUV involved in the December 2015 San Bernardino terrorist attack.*

Clapper said any attempted attack in the U.S. would echo the Europe assaults and, as in those cities, ISIS would "either infiltrate people or incite people who are already here." In a reference to the December 2015 shootings in San Bernardino, Calif., he added, "we've already seen some cases of that."

## Terror spread 'cause for serious concern'

U.S. officials' concerns are not unfounded. There was a 650 percent increase in fatal terror attacks on people living in the world's biggest economies over

**Figure 5.** Example Stimulus.

CNN

## US says 75% of ISIS fighters killed

**By Christine Crowell, CNN**

**(CNN)** - At least 75% of ISIS fighters have been killed during the campaign of US-led airstrikes, according to US officials.

The US anti-ISIS envoy said the campaign has winnowed ISIS' ranks to between 12,000 and 15,000 "battle ready" fighters, a top US official said.

The figures mean the US and its coalition partners have taken out vastly more ISIS fighters in Iraq and Syria than currently remain on the battlefield, two years since the bombing campaign began. Last week a US official said the coalition had killed 50,000 militants since 2014.

CIA Director John Brennan participates in a session at the 3rd annual Intelligence and National Security Summit in Washington, DC

Speaking at the White House, Brett McGurk, the US special envoy to the anti-ISIS coalition, said the terror group is no longer able to replenish its ranks, predicting the number of fighters would continue to dwindle.

The Obama administration has been in "relentless pursuit" of ISIS, John Brennan, director of the Central Intelligence Agency, told CNN.

Brennan touted the administration's efforts against terrorist groups, which include a coalition of more than 60 countries to attack ISIS's financial and oil infrastructure, stemming the flow of foreign fighters joining them in Syria and Iraq, and training Iraqi and Kurdish soldiers to help in the battle.

### The fear appeal message

This study furthers privacy research by using EPPM to determine to what extent participants are willing to waive privacy rights and allow for increased government surveillance. In furtherance of that goal, this study tests EPPM in relation to the threat of terrorism, compares two high efficacy options to determine if there are significant differences, and examines the effect of cognitive dissonance on threat, efficacy and privacy concern. As noted previously, each article was manipulated based on threat level and type of efficacy. For example, some of the articles contained an efficacy message that advocated for increased government surveillance of

phone and Internet communications in order to combat terrorism. Other articles contained an efficacy message that advocated for relying on individual reporting of suspicious activity to law enforcement to fight terrorism (see Table 1). Articles using specific combinations of independent variables (*i.e.* high threat/low efficacy; high threat/high efficacy increased governmental surveillance; and high threat/high efficacy individual reporting) were randomly assigned to each experimental group.

**Table 1.** Experimental Groups

| **Group** | **Topic** | **High/Low Threat** | **High/Low Efficacy** |
|---|---|---|---|
| Group 1 | Government Surveillance | High Threat | High Efficacy |
| Group 2 | Government Surveillance | High Threat | Low Efficacy |
| Group 3 | Individual Reporting | High Threat | High Efficacy |
| Group 4 | Individual Reporting | High Threat | Low Efficacy |
| Group 5 | Government Surveillance | Low Threat | High Efficacy |
| Group 6 | Government Surveillance | Low Threat | Low Efficacy |
| Group 7 | Individual Reporting | Low Threat | High Efficacy |
| Group 8 | Individual Reporting | Low Threat | Low Efficacy |
| Group 9 | Control Group | NA | NA |

Witte (1993; Witte et al., 1998) published instructions regarding what elements are necessary for a good fear appeal. While other scholars have relied on Witte's (1993; Witte et al., 1998) recommendations when crafting fear appeals for similar studies (Goodall & Reed, 2013; McMahan, Witte & Meyer, 1998; Morman, 2000; Muthusamy, Levine & Weber, 2009; Roskos-Ewoldsen, Yu & Rhodes, 2004; Smith et al., 2008, and Witte & Allen, 2000), their research does

not offer the same level of detailed instruction about the specific fear appeal elements. Thus, the fear appeal in this study was structured as per Witte's (1993; Witte et al., 1998) specific recommendations. Witte (1993; Witte et al., 1998) suggests that fear appeals need to be created systematically. Fear appeals must contain certain "(a) structural, (b) stylistic, and (c) extra-message features" (Witte, 1993, p. 147; Witte et al., 1998). When it comes to structure, the fear appeal must present both a threat and a recommended avenue to minimize or prevent the threat (efficacy) (Witte, 1993; Witte et al., 1998). The threat portion of the message must address both severity and susceptibility (Witte, 1993; Witte et al., 1998). The efficacy portion needs to include response efficacy and self-efficacy (Witte, 1993; Witte et al., 1998). Finally, extra-message relates to features that might be able to influence the reader but are not explicitly part of the message such as source credibility (Witte, 1993; Witte et al., 1998). Witte (1993; Witte et al., 1998) proposed four procedures to develop an ideal fear appeal. First, when creating each component of the fear appeal (*i.e.* threat severity, threat susceptibility, self-efficacy, and response efficacy), the researcher must craft the language in order to address the particular audience (Witte, 1993; Witte et al., 1998). Second, the different fear appeal levels need to be manipulated through the substantive language (Witte, 1993; Witte et al., 1998). Thus, language that is meant to convey a high fear appeal will emphasize how severe the threat is, be "vivid and intense," and focus on the susceptibility of the reader (Witte, 1993, p. 148; Witte et al., 1998). Conversely, low fear appears will use neutral language and be vague about the risk to the audience (Witte, 1993; Witte et al., 1998). Third, the different levels of fear appeals need to be comparable (Witte, 1993; Witte et al., 1998). In other words, the sources, accuracy and complexity must be the same (Witte, 1993; Witte et al., 1998). Fourth, the message needs to be targeted to the correct audience and the efficacy options need to correspond with the variables being tested (Witte, 1993; Witte et

al., 1998). This means that if the efficacy calls for specific action from the reader then the variables being measured need to also address specific action (Witte, 1993; Witte et al., 1998). Witte (1993; Witte et al., 1998) suggests using a single-message design when studying fear appeals.

Following Witte's (1993; Witte et al., 1998) instruction, a high-threat fear appeal message was developed pertaining to terrorism. The message focused on a general, American adult audience's susceptibility to terrorism and the severity or risk of it. The messaged focused on the possibility of a terrorist attack in the United States and used vivid language to describe the severity of terrorism. The low threat message focused on the eradication of ISIS. Both messages were crafted using actual CNN articles as the base message (see Appendix B). The headlines and headings in both messages came from actual news sources. A professional journalist reviewed and edited the articles to ensure journalistic style and formatting.

The government surveillance high efficacy message focused on ways that surveillance can help root out and prevent terrorist activities. The language was taken from actual news stories and the NSA's website. The low efficacy message contained information that suggests government surveillance cannot stop terrorist attacks. The language and information were taken from real studies and news stories. The individual reporting high efficacy message focused on the effectiveness of individual reporting of suspicious activity in order to stop terrorism. The language was taken from news articles and the FBI's website. The low efficacy option contained information suggesting that reporting suspicious activity to authorities does not stop terrorist attacks. This language was again taken from real news stories. All of the stimulus articles are provided in Appendix B.

**Measures**

The EPPM variables were measured using closed-ended questions adapted from measures used in previous research by Witte (2000). According to Witte's (1992; Witte, 2000) research, perceived threat, efficacy, danger control and fear control are made up of multiple components, which are combined to create scales. In this study, the internal reliability of the scale was measured using Cronbach's alpha. An alpha greater than .70 represents acceptable reliability, and a result greater than .80 represents strong reliability.

*Perceived threat.* The items used to measure threat were gathered from previous research by Witte, et al. (1996; Witte, 1994; Witte et al., 1998; McMahan, Witte and Meyer, 1998). Perceived threat includes two components: susceptibility and severity. As suggested by Witte, et al. (1996; Witte et al., 1998), three items were used to measure each component. The items were measured using a 7-point-Likert scale (1=strongly disagree to 7=strongly agree). All six items were averaged in order to create a scale ($\alpha = .82$) (See Table 2).

*Perceived efficacy.* There are two components to efficacy: self-efficacy and response efficacy. The items used to measure these components were measured using a 7-point-Likert scale (1=strongly disagree to 7=strongly agree). As suggested by Witte (2000; Witte, et al., 1996; Witte et al., 1998), three items were used to measure each type of efficacy (see Table 1). All of the items were averaged in order to create an efficacy scale. Because there were two separate efficacies that were tested in this study (increased government surveillance and individual reporting of suspicious activity), two distinct scales were calculated: Government surveillance efficacy ($\alpha = .93$) and individual reporting efficacy ($\alpha = .89$).

*Danger control/Message Acceptance.* The danger control variable (or message acceptance) consists of two variables: attitudes and intentions. Attitudes toward the two efficacy options

were measured using Witte (2000; Witte, 1994; Witte et al., 1996; Witte et al., 1998) procedure, which uses semantic differential scales. In this study, attitudes toward governmental surveillance ($\alpha = .95$) and individual reporting were measured using six semantic differential scales that were combined to create two separate scales (see Table 2). Intent was measured using three items that asked participants about their future intentions regarding the efficacy options (see Table 2). The items were measured using a 7-point-Likert scale (1=strongly disagree to 7=strongly agree). The items were averaged to create two new scales: Intent (individual reporting) ($\alpha = .88$) and Intent (government surveillance) ($\alpha = .87$)

*Fear control/Message Rejection.* Fear control, which is made up of three components, was measured using items developed by Witte (2000; Witte, 1994; Witte et al., 1996; Witte et al., 1998). The three components are: Defensive avoidance, message minimization and message manipulation.

Defensive avoidance was measured by asking participants to respond to three items pertaining to terrorism, which were measured using 7-point Likert scales (see Table 2). The items were averaged in order to create an avoidance scale ($\alpha = .90$).

Message minimization examines reactance (Witte, 2000, Witte, 1994; Witte et at., 1998). In other words, it measures how much an individual minimizes the message contained in the fear appeal. Message minimization was measured by asking participants to rate adjectives on a 7-point Likert scale (1=strongly disagree to 7=strongly agree) (see Table 2). The items were averaged in order to create a minimization scale ($\alpha = .96$).

Perceived manipulation was measured by asking participants to rate adjectives pertaining to how they felt about the article they read (see Table 2). The items were measured on a 7-point

Likert scale (1=strongly disagree to 7=strongly agree) and were averaged to in order to create a manipulation scale ($\alpha = .94$).

*Fear.* The final EPPM variable is fear, which was measured by having the participants rate adjectives that describe how frightened or uncomfortable they felt after reading the article (Witte, 2000; Witte, 1994) (see Table 2). The items were measured using a 7-point-Likert scale (1=not at all to 7=very much) and then averaged in order to create a fear scale ($\alpha = .95$).

In addition to testing the EPPM variables, this study sought to discover if cognitive dissonance was associated with message rejection and if there is a relationship between acceptance of increased government surveillance and privacy concern. Thus the following variables were created.

*Cognitive dissonance*. Metzger, Hartsell and Flanagin (2015) determined that previous cognitive dissonance studies assumed dissonance was present but did not actually measure for it, so they developed a new scale to specifically measure participants' cognitive dissonance. This current study used items adapted from the Metzger *et al.* (2015) study. Nine items, each measured using a 7-point Likert scale (ranging from 1=strongly disagree to 7=strongly agree), were used to measure dissonance. However, one item was subsequently removed due to reliability concerns (see Table 2). With that item included, the reliability alpha was .77; however, after removing that item, the alpha increased to .79. The eight items, shown in Table 1, were averaged in order to create a dissonance scale.

*Privacy concern.* The items used to measure privacy attitude were gathered from previous research by Buchanan, Paine, Joinson, and Reips (2007). Buchanan et al. (2007) developed three scales to measure people's behaviors and attitudes toward privacy. Two of the scales were

behavioral in nature: general caution scale and technical protection scale (Buchanan et al., 2007). The third scale, called the privacy concern, measured people's attitudes. The privacy concern scale contained 16 items. This current study used seven items adapted from the Buchanan *et al.* (2007) study (see Table 2). The items were measured using a 7-point-Likert scale (1=not at all to 7=very much). All of the items were averaged in order to create a privacy concern scale ($\alpha = .79$).

*General attitude toward Government*. Because this study relates to national security and government surveillance, it was important to measure each participants' attitude toward the current U.S. government. The items used to measure attitude toward the government were adapted from Witte's (2000; Witte 1994; Witte et al., 1996; Witte et al., 1998) EPPM attitude scale. This variable was measured using uses six semantic differential scales (see Table 1). The items were then averaged in order to create a government attitude scale ($\alpha = .96$).

**Table 2.** Variables, items, means and standard deviations

| Variable | Items | α | Mean* | Standard Deviation |
|---|---|---|---|---|
| **Perceived Threat** | | .82 | 5.09 | .99 |
| | Perceived Susceptibility<br>• It is likely that I will be a victim of terrorism.<br>• It is possible that I will be a victim of terrorism.<br>• I am at risk of being a victim of terrorism. | .87 | 4.12 | 1.31 |
| | Perceived Severity<br>• I believe the risk of terrorism is serious<br>• I believe the risk of terrorism is significant<br>• I believe the risk of terrorism is severe. | .83 | 6.1 | 1.07 |
| **Government Surveillance Efficacy** | | .93 | 4.33 | 2.99 |
| | Response Efficacy | .93 | 4.38 | 1.50 |

| | | | | |
|---|---|---|---|---|
| | • Government surveillance of phone and Internet communications works to prevent terrorism.<br>• Government surveillance of phone and Internet communications is effective in preventing terrorism.<br>• If government surveillance of phone and Internet communications is increased, I am less likely to be affected by terrorism.<br>• Increased government surveillance of phone and Internet communications is important to combat the threat of terrorism. | | | |
| | Self-Efficacy | .91 | 4.26 | 1.57 |
| | • I am able to allow increased government surveillance of phone and Internet communications in order to prevent terrorism.<br>• Allowing increased government surveillance is easy to do in order to prevent terrorism.<br>• Allowing increased government surveillance to prevent terrorism is convenient. | | | |
| **Individual reporting Efficacy** | | .89 | 5.20 | 1.10 |
| | Response Efficacy | .86 | 5.13 | 1.21 |
| | • Individual reporting of suspicious activity to law enforcement works to prevent terrorism.<br>• Individual reporting of suspicious activity to law enforcement is effective in preventing terrorism.<br>• If I report suspicious activity to law enforcement, I am less likely to be affected by terrorism.<br>• Individual reporting of suspicious activity is important to combat the threat of terrorism. | | | |
| | Self-Efficacy | .85 | 5.36 | 1.18 |
| | • I am able to report suspicious activities to law enforcement in order to prevent terrorism.<br>• Reporting suspicious activity to law enforcement is easy to do in order to prevent terrorism.<br>• Reporting suspicious activity to law enforcement to prevent terrorism is convenient. | | | |

| | | | | |
|---|---|---|---|---|
| **Intent (Government surveillance)** | • I intend to consent to increased government surveillance of phone and Internet communications in order to help prevent terrorism.<br>• I intend to contact my state and federal legislators about increasing government surveillance in order to help prevent terrorism.<br>• I intend to talk to my friends about allowing increased government surveillance in order to combat terrorism. | .87 | 3.83 | 1.64 |
| **Attitudes (Government surveillance)** | Semantic differential scales: bad-good; undesirable-desirable; unfavorable-favorable; not effective-effective; and disapprove-approve. | .95 | 4.41 | 1.72 |
| **Intentions (Individual Reporting)** | • I intend to report suspicious activity to law enforcement in order to help prevent terrorism.<br>• I intend to contact law enforcement if I see an individual acting suspicious.<br>• I intend to talk to my friends about contacting law enforcement to help prevent terrorism. | .88 | 5.22 | 1.10 |
| **Attitudes (individual reporting)** | Semantic differential scales: bad-good; undesirable-desirable; unfavorable-favorable; not effective-effective; and disapprove-approve. | .94 | 5.74 | 1.26 |
| **Cognitive Dissonance** | • I regret reading this news story.<br>• CNN as a news source makes me uncomfortable<br>• I disliked reading this news story.<br>• I agreed with the stance taken in this news story. (reverse coded)<br>• I felt uncomfortable while reading this news story.<br>• I enjoyed reading this news story. (reverse coded)<br>• I like CNN as a news source. (reverse coded)<br>• This story made me question my own beliefs. (removed)<br>• I disliked the topic of this news story | .79 | 3.24 | 1.08 |
| **Defense avoidance** | • I tend to avoid thoughts about terrorism.<br>• I try not to think about terrorism.<br>• I avoid discussing terrorism with friends and family. | .90 | 4.06 | 1.60 |

| | | | | |
|---|---|---|---|---|
| **Message Minimization** | • This article was: [exaggerated]; [distorted], [overblown], and [overstated]. | .96 | 3.27 | 1.50 |
| **Perceived Manipulation** | • This article was: [manipulative], [misleading], [exploitative].<br>• This article tried to manipulate me. | .94 | 3.22 | 1.50 |
| **Fear** | • How much did this article make you feel: [frightened]; [tense]; [nervous]; [anxious]; [uncomfortable]; [nauseous]. | .95 | 2.82 | 1.59 |
| **Privacy concern** | • In general, how concerned are you about your privacy while you are using the Internet?<br>• In general, how concerned are you about your privacy while talking on your phone or cellphone?<br>• Are you concerned about people you do not know obtaining personal information about you from your online activities?<br>• Are you concerned that an email you send may be read by someone else besides the person you sent it to?<br>• Are you concerned that an email you send someone may be inappropriately forwarded to others?<br>• Are you concerned about online identity theft?<br>• Are you concerned who might access your personal.929 records electronically? | .92 | 4.62 | 1.53 |
| **General Attitude toward U.S. Government** | Semantic differential scales: bad-good; disapprove-approve; unfavorable-favorable; not effective-effective; and untrustworthy-trustworthy. | .96 | 3.86 | 1.57 |

**Note: All of the items were scored using a seven-point Likert-type scale.*

Participants were asked two additional yes/no items regarding their experiences with terrorism or online identity theft. Because this study focused on online surveillance and privacy, the question about identity theft was used as a control variable to determine if privacy concern was impacted by identity theft. More specifically, participants were asked if they (or anyone close to them) had been a victim of terrorism or identity theft. Finally, participants were asked

demographic questions pertaining to age, gender, education, political affiliate and race/ethnicity. This study, including all of the measures/items and stimuli contained in appendix A, were reviewed and approved by an Institutional Review Board (IRB) before the experiment was conducted.

Three manipulation tests were conducted to ensure that the threat, efficacy and fear variables were being manipulated properly. The first manipulation test was conducted on the nine stimulus articles. For this test, 36 respondents were recruited, using a mix of convenience and snowball sampling of students at a mid-sized university located in the Northeastern United States. Though the results were not significant, the test did indicate that the high threat groups were perceiving an increased threat as compared to the other groups and the high efficacy groups were perceiving an increased efficacy as compared to the other groups. A second manipulation test was conducted during a pretest of the experiment. The pretest had sixty-six respondents who were recruited through Amazon's Mechanical Turk. Respondents were randomly placed into one of the eight experimental groups or the control group. To test the manipulation of the threat variable, a Kruskal-Wallis test was conducted using the threat level (high/low/control) as the between-subjects factor and level of perceived threat as the dependent variable. The result was not statistically significant ($x^2$ (2, n = 66) = 2.61, ns). The means appeared to be heading in the right direction, but there was only a slight difference between the groups. The groups with a high threat manipulation had a perceived threat mean of 4.49 (SD = 1.18), which was marginally higher than the groups who received the low threat manipulation (M = 4.22, SD = 1.26) and the control group (M = 4.0, SD = .97). Another Kruskal-Wallis test was conducted using the efficacy level (high/low/control) as the between-subjects factor and level of perceived efficacy as the dependent variable. To check the efficacy at this level, an overall composite of efficacy was

created, combining both government surveillance efficacy and individual reporting efficacy variables (α = .91). The result was not statistically significant ($x^2$ (2, n = 66) = 3.12, ns). The groups who received the high efficacy manipulations had a perceived efficacy mean of 4.34 (SD = 1.12), which was higher than the groups who received the low efficacy manipulations (M = 3.92, SD = 1.10). However, the high efficacy group was not higher than the control group (M = 4.38, SD =.88), which suggested that the efficacy in the high efficacy stimulus articles should be adjusted to ensure a sufficient manipulation. In addition, Witte (1998) suggests that there is a positive correlation between perceived fear and threat, where increased perceived threat will result in increased fear. A Spearman correlation showed that there was a statistically significant positive correlation between fear and perceived threat ($r_s$ = .49, n = 66, p <.05). Overall, the results indicated that the means were moving in the correct direction, but most were not yet significant. This could have been the result of the small sample size. The stimulus articles was modified with changes to substantive content and headings to help increase the effects of the manipulations. Specifically, the wording of the headings was changed to more precisely accentuate the levels of threat and efficacy. The size of the headings was also enlarged, to help draw readers' attention. Some of the wording in the stimulus articles was revised to better highlight the threat and efficacy manipulations. The third, and final, manipulation check was conducted during the experiment, which is described in detail later in this study.

During the pretest, the variable scales were tested for reliability. All of the scales were found to be reliable: threat severity α = .85; threat susceptibility α = .81; response efficacy government surveillance α = .94; self-efficacy government surveillance α = .89; response efficacy individual reporting α = .91; self-efficacy government surveillance α = .86; attitude toward government surveillance α = .90; attitude toward individual reporting α = .93; intent

toward government surveillance α = .84; intent toward individual reporting α = .86; avoidance α = .70; minimization α = .98; manipulation α = .95;  fear α = .96; dissonance α = .77; and privacy concern α = .96. The avoidance scale was close to being unreliable, so one of the items was changed, using Witte's (2000) list of avoidance items.

# Chapter 5: Results

This chapter offers an in-depth explanation of the manipulation check and the results for each of the hypotheses. A variety of statistical analyses were used including, Kruskal-Wallis, Mann-Whitney U, Spearman correlation, hierarchical multiple regression and path analysis. Nonparametric statistical tests were used because the variable normality was not present. The betas reported in these results are all standardized.

## Manipulation and Validity Checks

As noted, the third manipulation check was conducted during the experiment to test that the threat, efficacy and fear variables were properly manipulated. For the threat variable, a Kruskal-Wallis test was conducted using the threat level (high/low/control) as the between-subjects factor and level of perceived threat as the dependent variable. The groups with a high threat manipulation had a perceived threat mean of 5.23 (SD = .94), which was higher than the groups who received the low threat manipulation (M = 5.03, SD = .98). It was also higher than the control group (M = 4.78, SD = 1.14). This result was statistically significant ($x^2$ (2, 360) = 6.71, $p < .05$). The means were not as different as the researcher expected them to be. The post hoc Tukey test indicated that the high threat groups perceived a significantly higher level of threat than the control group but was not significantly different from the low threat level groups. This result could have an impact on the EPPM-related tests. However, EPPM suggests that high perceived threat and high perceived efficacy will lead an individual toward a danger control response, while high perceived threat and low perceived efficacy will result in a fear control response. This can still be tested even if the perceived threat levels are high in all of the groups.

Another Kruskal-Wallis test was conducted using the efficacy level (high/low/control) as the between-subjects factor and level of perceived efficacy as the dependent variable. To check

the efficacy at this level, an overall composite of efficacy was created, combining both of the government surveillance efficacy and individual reporting efficacy variables ($\alpha = .93$). The groups who received the high efficacy manipulations had a perceived efficacy mean of 4.97 (SD = 1.01), which was higher than the groups who received the low efficacy manipulations (M = 4.62, SD = 1.19) and the control group (M = 4.62, SD =1.10). This result was statistically significant ($x^2$ (2, n = 360) = 7.46, $p < .05$). Witte (1998) suggests that there is a positive correlation between fear and threat, where increased perceived threat will result in increased fear. A Pearson correlation suggested that this was the case here as well. There was a positive correlation between fear and perceived threat ($r_s = .41$, n = 360, $p < .05$). This result was as expected. However, the correlation was not as strong as it had been in the pre-test ($r_s = .49$, n = 66, $p < .05$), which could be a result of the different samples or sizes and composition of the samples.

Validity of each participants' responses were checked a few different ways during the experiment. Two attention check questions were inserted into the instrument, asking respondents to choose a specific response. If participants responded incorrectly, that participant was dropped from the experiment and was randomly replaced by a new participant. In addition, the time it took for each participant to read the stimulus article and complete the survey instrument was monitored. The average time for participants to complete the survey was calculated, and any participant who finished the survey in one-third of the time or less than the average was removed from the experiment and randomly replaced with a new participant. These checks helped to ensure that the collected responses were valid.

*Sample*

The sample (N = 360) was 22.8% males, 76.7% females, with a mean age of 39.48 years. Approximately 81% of the participants reported that they are "white." The participants reported political and educational diversity (see Table 3). Though the mean age of the sample was close to 40, the majority of the sample was under 45, which is young. However, there is no evidence from the statistical analyses that age is a confounding variable in relation to any of the key variables.

**Table 3.** *Respondent Characteristics*

| Characteristics | Percent for all respondents (N = 360) |
|---|---|
| Gender | |
| Male | 22.8% |
| Female | 76.7% |
| Choose not to identify | .6% |
| Hispanic or Latino (of any race) | 10.8% |
| Ethnicity/race | |
| African American | 10.0% |
| White | 81.4% |
| Asian/Pacific Islander/other | 8.6% |
| Highest level of education | |
| High school degree or some high school | 29.7% |
| Some college | 22.8% |
| Associates degree or Trade/Vocational | 19.4% |
| Bachelor's degree | 20.8% |
| Master's degree or more advanced degree | 7.2% |
| Political Affiliation | |
| Democrat | 31.1% |
| Republican | 30.6% |
| Independent/other | 38.3% |
| Age | |
| 18-25 | 13.3% |

| | |
|---|---|
| 26-35 | 33.3% |
| 36-45 | 21.1% |
| 46-55 | 16.9% |
| 56 and above | 13.9% |
| No response | 1.4% |

**Hypotheses and Research Question Testing**

Because of the lack of diversity with gender and race, a series of chi-square tests were conducted to determine if there were any statistically significant differences between the experimental groups based on gender and race. No significant difference was found. Multiple two-way ANOVAs were also run to determine whether gender and race had any main or interactive effects on the key dependent variables, but no significant differences were found. In addition, an ANOVA was run to determine whether age had a significant effect on any of the variables. Age was broken into five groups (Group 1: 18 – 25; Group 2: 26 – 35; Group 3: 36 – 45; Group 4: 46 – 55; and Group 5: 56 and older). A significant result was found as to general attitudes toward the government. The difference was between Group 1 ($M = 4.31$, $SD = 1.52$) and Group 5 ($M = 3.43$, $SD = 1.59$). General attitudes toward the government is not a key EPPM variable, so the significance is not a cause for concern. However, any analyses looking specifically at that variable were controlled for age. Additional chi-square tests and ANOVAs were conducted to determine if there were statistically significant difference among the experimental condition grounds for the other demographic and descriptive variables including, age, education, political affiliation, general attitude toward the government, whether the participant had been a victim of terrorism, and whether the participant had been a victim of cyber-theft. No significant difference was found across the groups.

*Hypothesis 1*

Hypothesis 1a, proposing that participants exposed to the high threat/high efficacy government surveillance fear appeal would be more likely to choose the danger control route and accept the message than those exposed to the high threat/low efficacy government surveillance fear appeal, was not supported. Danger control is comprised of two variables, attitude and intent. The items from those variables were combined to form a composite danger control scale ($\alpha$ = .94, M = 4.25, SD = 1.60). A Kruskal-Wallis Test showed no significant differences in the danger control level among the designated groups ($\chi^2(2) = 1.66$, ns).

A post-hoc Kruskal-Wallis Test was conducted to see if either of the two dependent variables (attitude and intent) was significantly different between the groups. The results were not significant for attitudes ($\chi^2(2) = 1.61$, ns) or intent ($\chi^2(2) = 2.60$, ns).

Hypothesis 1b, proposing that participants exposed to the high threat/high efficacy individual reporting fear appeal would be more likely to choose the danger control route than those exposed to the high threat/low efficacy fear appeal and the control group, was not supported ($\chi^2(2) = .45$, ns). A post-hoc Kruskal-Wallis test was conducted to see if either of the two danger control variables was significantly different between the high threat individual reporting groups or the control group. The results were not significant for attitudes ($\chi^2(2) = .28$, ns) or intent ($\chi^2(2) = .97$, ns).

Because the EPPM hypotheses were not supported, additional post-hoc analysis offered a closer examination of the EPPM variables. Some research suggests that the best predictors of whether a message will be accepted are response efficacy and self-efficacy (Roskos-Ewoldsen, et al, 2004; Floyd, Prentice-Dunn, & Rogers, 2000). To test this, a sequence of simple regressions was conducted to determine how much each variable can predict danger control. The control

group was removed from this analysis because there was no efficacy option in the control group stimulus, and the control group answered items that responded to both efficacy options. The first simple regression found that threat ($\beta = .21$, $p < .05$), which is threat severity and susceptibility combined (see Table 2), can predict 4.6% of the variance in danger control ($F(1,318) = 15.18$, $p < .05$). The second simple regression found that efficacy ($\beta = .84$, $p < .05$), which is response efficacy and self-efficacy combined (see Table 2), can predict 72% of the variance in danger control ($F(1, 318) = 817.21$, $p < .05$).

Research also suggests that the level of threat is a better predictor of fear control than efficacy (Roskos-Ewoldsen, et al, 2004). To test this, a sequence of simple regressions was conducted to determine how much each variable can predict fear. The first simple regression found that threat ($\beta = -.17$, $p < .05$) can predict three percent of the variance in fear control ($F(1,318) = 9.36$, $p < .05$). The second simple regression found that efficacy ($\beta = -.08$, $p < .05$) can predict .6 percent of the variance in fear control ($F(1, 318) = 1.92$, $p < .05$).

*Research question 1*

Research question 1 sought to determine if the danger control rate of the participants exposed to the government surveillance high efficacy option was different from the danger control rate of participants exposed to the individual reporting efficacy option. For this analysis, the danger control variables, attitude and intent, for each efficacy group (government surveillance/individual reporting were combined into one danger control variable ($\alpha = .95$, $M = 4.97$, $SD = 1.57$). The 40 participants from the control group were not included in this analysis for two reasons. First, they were not offered an efficacy option in their stimulus article. Second, they answered items on both efficacy options, so they cannot be separated by the efficacy topic. Then, a Mann-Whitney U test was conducted with the efficacy topic (*i.e.*, government

surveillance/individual reporting) as the independent variable. The results showed that the danger control median for the individual reporting group (Md = 5.87, M = 5.75, SD = 1.07) was significantly higher than the danger control median for the government efficacy group (Md = 4.25, M = 4.20, SD = 1.61; U = 20081, z = 8.80, $p < .05$). The results indicate a moderate effect size ($r = .49$).

*Hypothesis 2*

There was no support for hypothesis 2a, proposing that participants exposed to the government surveillance high efficacy option would have more favorable attitudes toward government surveillance than those who were not (including the control group) ($\chi^2(8, n = 360) = 7.2$, ns). Hypothesis 2b, which isolated participants with an increased level of privacy concern, proposed that participants who were exposed to the government surveillance high efficacy option would have more positive attitudes toward government surveillance than participants exposed to other messages and the control group. This hypothesis was not supported ($\chi^2(8, n = 154) = 7.2$, ns).

There was support for hypothesis 2c, proposing that there would be a positive relationship between the perceived threat of terrorism and attitudes toward government surveillance of phone and internet communications. The relationship between the two variables was tested using Spearman correlation. There was a moderate, positive correlation between threat and attitudes toward government surveillance ($r_s = .32$, $n = 360$, $p < .05$), which means that high levels of perceived threat are associated with more positive attitudes toward government surveillance. When isolating the response based on the efficacy topic, the statistical significance remained: government surveillance ($r_s = .22$, $n = 160$, $p < .05$), individual reporting ($r_s = .39$, $n = 160$, $p < .05$) and control group ($r_s = .46$, $n = 40$, $p < .05$). A test of the statistical significance

between the government surveillance and individual reporting coefficients was not significant ($z = -1.74$, $p > .05$).

*Research Question 2*

Research question 2 asked if there was an association between the level of privacy concern and attitudes toward government surveillance for the entire sample. The relationship between the two variables was tested using Spearman correlation. The results showed no statistical relationship ($r_s = -.01$, $n = 360$, ns).

Because no statistical relationship was found between privacy concern and attitudes toward government surveillance, a post-hoc test was conducted to investigate the relationship between the variables further. The privacy concern variable was divided into two groups (high privacy concern and low privacy concern) to examine if there was a statistically significant difference between the groups based on concerns about privacy. It is logical that those who have a higher privacy concern will have more negative attitudes toward government surveillance. The Likert scale used to measure the privacy concern items used 7-points (none at all, very little, a little, a moderate amount, a lot, a great deal, very much). Those respondents who had a privacy concern mean that corresponded with "a moderate amount" and less (*i.e.*, 4.99 and below) were placed in the low privacy concern group. Responses with a privacy concern mean that corresponded with "a lot" and above (*i.e.* 5.0 and above) were placed in the high privacy concern group. The privacy concern mean for the low group was 3.52, while the mean for the high group was 6.09. Interestingly, the attitude toward government surveillance mean for the low privacy concern group was 4.44, while the mean for the high group was 4.37. Though the privacy concern means were quite different, the attitude toward government surveillance was basically the same, and a Mann-Whitney U test indicated that the difference between the groups was not

statistically significant (U = 16,018, z = .16, ns). There was no significant correlation between privacy concern and attitudes toward government surveillance in the high ($r_s$ = -.11, n = 154, ns) or low ($r_s$ = .05, n = 206, ns) privacy concern groups.

It is also logical that there would be a relationship between level of privacy concern and intent to allow increased government surveillance. However, a post hoc Spearman's rho indicated that there was no significant relationship between the two variables ($r_s$ = .04, n = 360, ns). The respondents were again divided in to high/low privacy concern groups to examine whether there were statistically significant differences between the groups. The low privacy concern group had an intent to allow government surveillance mean of 3.89, while the high group had a mean of 3.74. A Mann-Whitney U test indicated that there was no significant difference between the groups (U = 13,339, z = .93, ns).

*Hypothesis 3*

For the analysis, of hypotheses 3a and 3b, the fear control variables (avoidance, manipulation and minimization) were combined to form a composite fear control variable ($\alpha$ = .91, M = 10.53, SD = 3.52). Hypothesis 3a, which proposed that within the government surveillance groups, privacy concern and fear control would have a positive correlation, was unsupported ($r_s$ = .06, n = 160, ns).

Hypothesis 3b, proposing that within the individual reporting group, privacy concern and fear control would have a positive correlation, was supported. The result indicated that the level of privacy concern had a significant positive correlation with fear control ($r_s$ = .19, n = 160, $p < .05$). Interestingly, this result suggests that as privacy concern increased, message rejection about the effectiveness of reporting suspicious activities to authorities increased. In other words, the message, to be accepted or rejected, was that individual reporting of suspicious activity can help

combat terrorism. In this case, the results suggest that the higher the participants' privacy concern, the more likely that an individual would be to reject the message that reporting suspicious activity to authorities helps to fight terrorism.

This result led to the question: As privacy concern increases, will the respondent be less likely to contact authorities to report suspicious activity? Looking specifically at the individual reporting group, a Spearman correlation was conducted to determine the relationships between privacy concern, attitudes toward individual reporting of suspicious activities to authorities, and the intent to report suspicious activity. There was not a significant relationship between privacy concern and attitudes toward individual reporting ($r_s$ = .001, n = 160, ns). However, there was a weak positive relationship between privacy concern and intent to report suspicious activity ($r_s$ = .18, n = 160, p <.05). This would suggest that as privacy concern increases, the likelihood of contacting authorities regarding suspicious activity also increases.

Post-hoc analyses were conducted to further investigate these results with the entire sample. There was again a weak positive relationship between privacy concern and the intent to report suspicious activity ($r_s$ = .17, n = 360, p < .05). There was no significant relationship between privacy concern and attitudes toward reporting suspicious activity ($r_s$ = .17, n = 360, p < .05).

*Research Questions 3 and 4*

Research questions 3 and 4 asked if dissonance was related to each of the EPPM variables. In order to conduct this analysis, the response efficacy items for government surveillance and individual reporting were averaged to create a single scale (α = .91, M = 4.77, SD = 1.44). The same was done for the self-efficacy items. However, for self-efficacy, the first question "I am able to [allow increased government surveillance/report suspicious activity] in

order to prevent terrorism" had to be removed to make the scale reliable (α = .89, M = 4.95, SD = 1.57). For this analysis, the control group was removed because that group responded to items relating to both efficacy options. Spearman rho was used for this analysis because the distribution of the variables was not normal. According to the results, fear, response efficacy and self-efficacy had weak statistical relationships with dissonance (see Table 4).

**Table 4** *Correlation Matrix for Dissonance and the EPPM Variables*

| Scale | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1. Dissonance | -- | | | | | |
| 2. Threat Severity | -.09 | -- | | | | |
| 3. Threat Susceptibility | .05 | .40** | -- | | | |
| 4. Fear | .27** | .24** | .46** | -- | | |
| 5. Response Efficacy | -.13* | .24** | .15* | .13* | -- | |
| 6. Self-Efficacy | -.17** | .27** | .23* | .12* | .73* | -- |

Note: ** p < .01, * p < .05 (2-tailed).

*Research Question 5*

Research question 5a asked if there was a significant relationship between dissonance and fear control. To complete this analysis, all of the items for the fear control variables (avoidance, manipulation and minimization) were combined to form a composite fear control variable (α = .91, M = 10.53, SD = 3.52). For this analysis, the control group was omitted for the same reasons as previously mentioned, with the primary reason being that they answered items regarding both efficacy options. The relationship between the variables was measured using a Spearman correlation. There was a strong relationship between the dissonance and fear control, $r_s = .57$, n = 320, p<.001, indicating that when dissonance increases, message rejection increases.

Research question 5b asked if there was a significant relationship between dissonance and danger control. For this analysis, the danger control variables (attitude and intent) were combined to form a composite danger control variable (α = .95, M = 9.89, SD = 3.16). The relationship between the variables was measured using Spearman correlation. There was a weak,

negative relationship between dissonance and danger control, $r_s = -.21$, $n = 320$, $p < .001$, suggesting that when dissonance increases, message acceptance decreases.

Research question 5c asked whether dissonance can predict variance in fear control after controlling for fear, perceived threat and perceived efficacy. First, a simple regression found that dissonance ($\beta = .58$, $p < .05$) can predict 34% of the variance in fear control ($F (1,358) = 162.69$, $p < .05$). Next, a hierarchical multiple regression was conducted to test how much that number is decreased when controlling for the other EPPM variable. Four outliers were removed from the analysis because of issues with the Mahalanobis distances and standardized residuals. After their removal, preliminary analyses indicated that there were no violations of the assumptions of normality, multicollinearity, linearity and homoscedasticity. Each of the variables was entered separately to determine how much variance each explained. The results suggest that fear explained little of the variance in fear control, while dissonance explained the most variance. Model 4, which included all of the variables, explained 37 percent of the variance, $F (4, 311) = 47.14$, $p <.05$. Dissonance explained 30 percent of the variance in fear control after controlling for fear, perceived threat and perceived efficacy (see Table 5).

Next, Preacher and Hayes' (2008; Hong, 2011) bootstrapping method was used to determine whether dissonance would directly and indirectly affect fear control (message rejection) when mediated by threat severity, threat susceptibility, response efficacy and self-efficacy. Preacher and Hayes (2008) suggest that their bootstrapping analysis is superior to SOBEL when testing indirect effects in multiple mediator models. According to Preacher and Hayes (2008), Sobel's delta method is best used with "very large samples" that assume "multivariate normality" (p. 883). Preacher and Hayes (2008) found that in smaller samples, the total indirect effect is not always found; however, they suggest that a significant total indirect

effect is not required and that specific indirect effects are still noteworthy even if the total indirect effect is not significant. In addition, their bootstrapping method allows for multiple mediators (Preacher & Hayes, 2008). Preacher and Hayes (2008) created a macro syntax called "Indirect" that can be used with SPSS to determine indirect mediate effects. Their bootstrapping method is useful in that it uses a resampling technique where a sample of the cases taken from the full sample are used to create a new sampling distribution, or rather, an "empirical, nonparametric approximation of the sampling distributions of the indirect effects of interest" (Preacher & Hayes, 2008, p. 833; Hong, 2011). This method is useful because it does not rely on the assumption of a normal sampling distribution (Preacher & Hayes, 2008, Hong, 2011). This method also is known to reduce Type 1 error (Hong, 2011).

The results show dissonance has a negative relationship with threat severity, response efficacy and self-efficacy (see Figure 6 and Table 5). This means that as efficacy increases, dissonance decreases. Interestingly, it also means that as threat severity increases, dissonance decreases. The effect of dissonance on fear control without taking the other variables into account is significant (*path coefficient* =.58, SE =.05, p<.001.) When controlling for the mediating variables, the effect of dissonance on fear control remains significant (*path coefficient* =.56, SE =.05, p<.001) (see Figure 6). The results also indicate that threat severity and response efficacy are statistically significant as mediators because the bias-corrected 95% confidence intervals do not contain zero. The model explains 37 percent of the variance in fear control. According to the bias-correct 95% confidence intervals, the total indirect effect of the model is not significant (-.07 to .14).

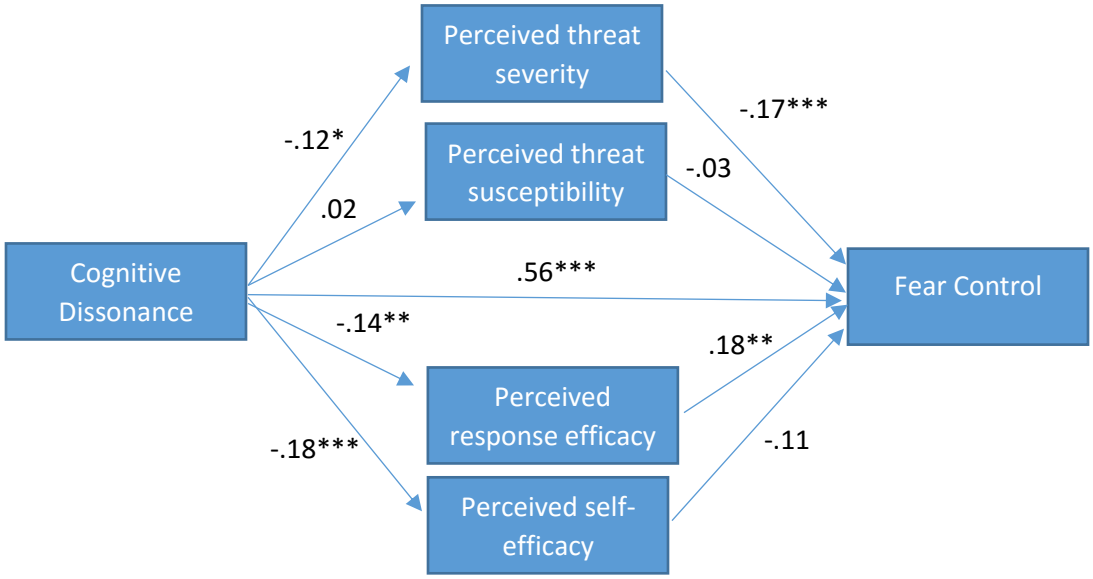



**Figure 6:** Relationship between cognitive dissonance, threat severity, threat susceptibility, response efficacy, self-efficacy and fear control (message rejection). Standardized coefficients are shown. Significance: ***p < .001, **p < .01, *p< .05.

**Table 5** *Results of Indirect Effects on Fear Control Using Bootstrapping*

| | Path coefficient | SE | Bias Corrected Bootstrap 95% confidence interval |
|---|---|---|---|
| Total effect of Dissonance on Fear Control | .58*** | .05 | |
| Dissonance to mediators | | | |
| Threat Severity | -.12* | .05 | |
| Threat Susceptibility | .02 | .06 | |
| Response Efficacy | -.14** | .07 | |
| Self-Efficacy | -.18*** | .07 | |
| Direct effects of mediators on Fear Control, controlling for Dissonance | | | |
| Threat Severity | -.17*** | .06 | |
| Threat Susceptibility | -.03 | .04 | |
| Response Efficacy | .18** | .05 | |
| Self-Efficacy | -.11 | .05 | |
| Direct effect of Dissonance on Fear Control | .56*** | .05 | |
| Indirect effects of Dissonance on Fear Control | | | |
| Threat Severity | .02 | .01 | .002 to .058 |
| Threat Susceptibility | -.00 | .00 | -.016 to .004 |
| Response Efficacy | -.03 | .01 | -.069 to -.005 |
| Self-efficacy | .02 | .01 | .000 to .060 |
| Total | .06 | .01 | -.017 to .052 |

*Note: ***p<.001, **p<.01, *p<.05. Total effect = The effect of Dissonance on Fear Control without taking the moderating variables into account. Direct effect = The effect of Dissonance on Fear Control when controlling for the moderating variables. Standardized coefficients are show.*

**Table 2** *Summary of Hierarchical Regression Analysis for Variables Predicting Fear Control*

| | Model 1 | | | Model 2 | | | Model 3 | | | Model 4 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Variable | B | SE b | β | b | SE b | B | b | SE b | β | b | SE b | β |
| Constant | 10.11 | .41 | | 15.07 | 1.09 | | 15.67 | 1.17 | | 8.19 | 1.14 | |
| Fear | .15 | .12 | .07 | .49 | .14 | .22** | .49 | .14 | .22*** | .08 | .12 | .03 |
| Threat | | | | -1.15 | .24 | -.31*** | -1.08 | .24 | -.29*** | -.81 | .20 | -.21*** |
| Efficacy | | | | | | | -.20 | .14 | -.08 | .07 | .12 | .03 |
| Dissonance | | | | | | | | | | 1.83 | .15 | .58*** |
| F Value | | 1.42 | | | 12.66*** | | | 9.13*** | | | 47.14*** | |
| $R^2$ | | .005 | | | .07 | | | .08 | | | .37 | |
| Adjusted $R^2$ | | .001 | | | .07 | | | .07 | | | .37 | |
| $R^2$ Change | | | | | .07 | | | .006 | | | .30 | |

*** p<.001; ** p<.01; * p<.05

Research question 5d asked whether dissonance can predict variance in danger control after controlling for fear, perceived threat and perceived efficacy. For this analysis, the danger control variables, attitude and intent, were combined to form a composite danger control scale ($\alpha$ = .94, M = 4.25, SD = 1.60). First, a simple regression found that dissonance ($\beta$ = -.21, $p < .05$) can predict four percent of the variance in danger control ($F(1,318) = 14.23$, $p < .05$). Next, a hierarchical multiple regression was conducted to test how much that number is decreased when controlling for the other EPPM variable. Eight outliers were removed from the analysis because of issues with the Mahalanobis distances and standardized residuals. After their removal, preliminary analyses indicated that there were no violations of the assumptions of normality, multicollinearity, linearity and homoscedasticity. Each of the variables was entered independently to determine how much of the variance each one explained. The results show that perceived efficacy explained the most variance. Model 4, which included all of the variables, explained 76 percent of the variance, $F(4, 307) = 249.20$, $p < .05$. Dissonance only explained an additional .3 percent of the variance in danger control after controlling for fear, perceived threat and perceived efficacy and was not statistically significant (see Table 8).

The Preacher and Hayes' (2008; Hong, 2011) bootstrapping method was used a second time to determine whether dissonance would directly and indirectly affect danger control (message acceptance) when mediated by threat severity, threat susceptibility, response efficacy and self-efficacy. As before, dissonance has a negative relationship with threat severity, response efficacy and self-efficacy (see Figure 7 and Table 7). The effect of dissonance on danger control without taking the other variables into account is significant (*path coefficient* =-.231, SE =.15, p<.001.) However, when controlling for the mediating variables, the effect of dissonance on danger control is no longer significant (*path coefficient* =-.05, SE =.08, ns.) (see

Figure 7). The results also indicate that response efficacy, and self-efficacy are statistically significant as mediators because the bias-corrected 95% confidence intervals do not contain zero. The model explains 72 percent of the variance in danger control. According to the bias-correct 95% confidence intervals, the total indirect effect of the model is significant (-.73 to -.16).

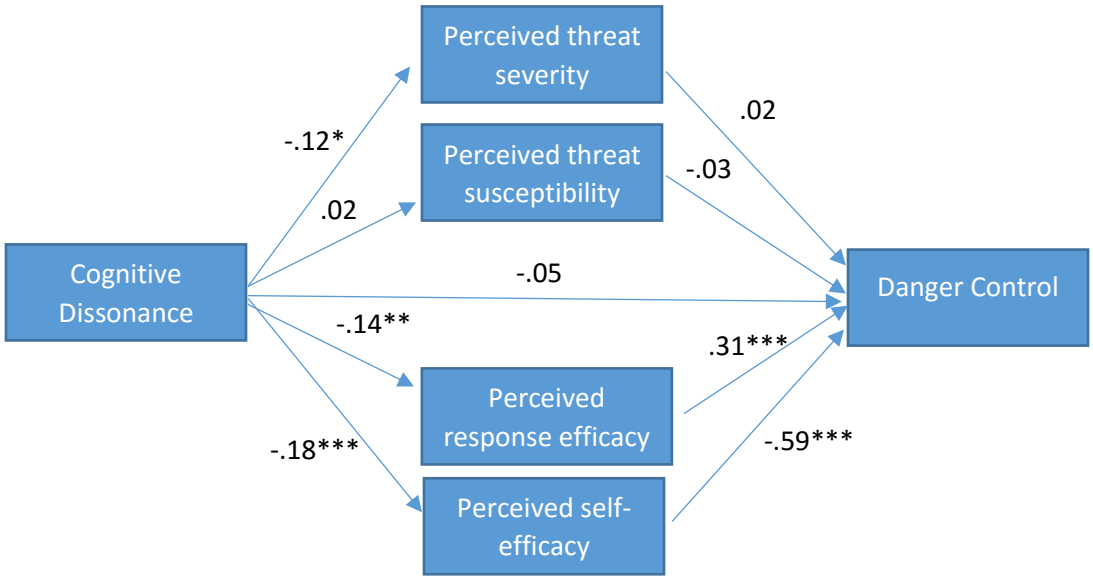



**Figure 7:** Relationship between cognitive dissonance, threat severity, threat susceptibility, response efficacy, self-efficacy and danger control (message acceptance). Standardized coefficients are shown. Significance: ***p < .001, **p < .01, *p< .05.

**Table 7** *Results of Indirect Effects on Danger Control Using Bootstrapping*

| | Path coefficient | SE | Bias Corrected Bootstrap 95% confidence interval |
|---|---|---|---|
| Total effect of Dissonance on Danger Control | -.21*** | .14 | |
| Dissonance to mediators | | | |
| Threat Severity | -.12* | .05 | |
| Threat Susceptibility | .02 | .06 | |
| Response Efficacy | -.14** | .07 | |
| Self-Efficacy | -.18*** | .07 | |
| Direct effects of mediators on Danger Control, controlling for Dissonance | | | |
| Threat Severity | .02 | .13 | |
| Threat Susceptibility | -.03 | .10 | |
| Response Efficacy | .31*** | .16 | |
| Self-Efficacy | .59*** | .17 | |
| Direct effect of Dissonance on Danger Control | -.05 | .14 | |
| Indirect effects of Dissonance on Danger Control | | | |
| Threat Severity | -.00 | .01 | -.04 to .01 |
| Threat Susceptibility | -.00 | .01 | -.03 to .01 |
| Response Efficacy | -.04 | .05 | -.27 to -.03 |
| Self-efficacy | -.10 | .10 | -.52 to -.11 |
| Total | -.14 | .14 | -.73 to -.16 |

*Note: ***p<.001, **p<.01, *p<.05. Total effect = The effect of Dissonance on Fear Control without taking the moderating variables into account. Direct effect = The effect of Dissonance on Fear Control when controlling for the moderating variables. Standardized coefficients are show.*

**Table 8** *Summary of Hierarchical Regression Analysis for Variables Predicting Danger Control*

| | Model 1 | | | Model 2 | | | Model 3 | | | Model 4 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Variable | B | SE b | β | B | SE | β | b | SE b | β | b | SE b | β |
| Constant | 4.71 | .18 | | 3.15 | .49 | | .25 | .26 | | .57 | .31 | |
| Fear | .11 | .05 | .11* | .01 | .06 | .01 | -.01 | .03 | -.01 | .004 | .03 | .004 |
| Threat | | | | .36 | .11 | .21** | .01 | .05 | -.01 | .003 | .05 | .002 |
| Efficacy | | | | | | | .97 | .03 | .87*** | .96 | .03 | .86*** |
| Dissonance | | | | | | | | | | -.07 | .04 | -.05 |
| F Value | 4.06* | | | 7.82*** | | | 328.61*** | | | 249.20*** | | |
| $R^2$ | .01 | | | .05 | | | .76 | | | .76 | | |
| Adjusted $R^2$ | .01 | | | .04 | | | .76 | | | .76 | | |
| $R^2$ Change | | | | .03 | | | .71 | | | .003 | | |

*** p<.001; ** p<.01; * p<.05.

*Hypothesis 5*

Hypothesis 5a proposed that, when isolating participants who were exposed to the government surveillance efficacy options, privacy concern would be associated with dissonance. This hypothesis was not supported ($r_s$ = .08, n = 160, ns). Because the eight experimental stimuli pertained to terrorism and some sort of government interaction through either individual contacting of government officials or through increased government surveillance, a post hoc analysis was conducted after combining the respondents of the experimental groups to determine if dissonance was associated with privacy concern. The results indicated that there was a weak positive relationship between the variables ($r_s$ = .12, n = 320, $p < .05$).

Because inconsistencies between beliefs and intent can cause dissonance, a post-hoc analysis was conducted to test the following hypothesis: Privacy concern and intentions to allow government surveillance will predict dissonance. A multiple regression was conducted to test this hypothesis, and the results were statistically significant. Privacy concern and intention to allow government surveillance explained 5.7% of the variance in dissonance ($F (2, 357) = 10.82$, $p <.05$). Both privacy concern ($\beta = .14$, $p < .05$) and intent to allow government surveillance ($\beta = -.21$, $p < .05$) were significant.

Hypothesis 5b proposed that, when isolating the participants who were exposed to the government surveillance efficacy options, there would exist a negative relationship between attitudes toward government surveillance and dissonance. This hypothesis was supported. The relationship between the two variables was examined using Spearman correlation. The results showed a weak negative correlation between attitude toward the government and dissonance, r = -.24, n = 160, $p < .05$, illustrating that a negative attitude toward government surveillance was associated with increased dissonance within that group.

# Chapter 6: Discussion

This study sought to test the Extended Parallel Process Model (EPPM) using terrorism as the threat and two distinct efficacy options. In addition, a privacy concern variable was included to determine if attitudes toward privacy play a role in accepting or rejecting government surveillance to fight terrorism. This study tested the relationship between dissonance and message rejection and acceptance. Finally, this study examined whether dissonance and the privacy paradox were related. This section will discuss the results and theoretical implications.

## EPPM

EPPM suggests that when a person is exposed to a fear appeal that contains a high threat and high efficacy, the person will be more likely to accept the efficacy message as compared to those who are exposed to a high threat/low efficacy message (Witte, 1994; Witte et al., 1998). Thus, it is logical that when respondents were exposed to the high threat/high efficacy messages, they would be more likely to accept those messages. That was not the case, however, in this study. There were no significant differences among the groups. Although this result appears surprising, a possible explanation could be that the level of efficacy was not high enough to surpass the level of threat. Witte et al. (1994; 1998), proposed that persuasive influence happens when the level of perceived efficacy surpasses the level of the threat. In this study, the perceived threat severity mean for the entire sample was high: 6.07 out of a seven-point Likert scale. When combining threat severity and threat susceptibility, the mean for perceived threat was 5.09. However, the efficacy mean for the entire sample was 4.77 out of seven. It is possible that these levels of perceived threat and efficacy affected the results. For example, the high threat/high efficacy government surveillance group should, under EPPM, be more likely to accept the message, that government surveillance can effectively combat terrorism, as compared to the

other groups. That was not found in this study, likely because of the higher level of perceived threat and lower level of perceived efficacy. The results showed that the perceived threat mean for the high threat/high efficacy government surveillance group was 5.14 out of seven, while the efficacy mean was 4.55. If the efficacy level was not high enough to overcome the threat, then, under the assumptions of EPPM, the participants would not be persuaded to accept the fear appeal message.

The high threat level could be the result of the January 6, 2017, shooting at the Fort Lauderdale airport, where a gunman took the lives of five people. This shooting took place only a week before the experiment was conducted. With the attack being reported in the news, terrorism may have been on the participants' minds. It could also be the case that the participants consider terrorism to be a high threat in general. There is evidence that a pre-existing fear of the threat could affect the EPPM results. A study by Muthusamy, Levine, and Weber (2009) indicated that if a group of participants have high, preexisting fear regarding the topic of study, manipulating the levels of threat and efficacy will not have an impact on danger control and fear control responses. In other words, if the participants' fear of terrorism is already high, it is unlikely that their fear can be further increased. In the Muthusamy et al. (2009) study, participants had a high, preexisting fear of HIV/AIDS, and although the levels of threat were manipulated in the message stimuli, the participants in the high threat groups did not have significantly higher levels of fear as compared to the low threat and control groups. Muthusamy et al. (2009) discovered that, because fear of HIV/AIDS could not be further increased, manipulation of the threat level did not have a significant impact on the participants' attitudes and intentions toward condom use to avoid contracting the disease. Moreover, Muthusamy et al. (2009) found that manipulating levels of efficacy did not significantly impact attitudes and

intentions toward condom use. The authors suggested this could be because the fear of HIV/AIDS was already so high that it could not be surpassed by the efficacy of condom use (Muthusamy et al., 2009).

This study had a comparable result. Similar to the Muthusamy et al. (2009) study, the threat levels were high and manipulating efficacy did not impact the rate of message acceptance. If the participants already had a high pre-existing fear about terrorism, and believed the threat to be significant, it is likely that the level of efficacy could not overcome the level of threat in a way that would persuade the participants to choose the danger control process and accept the message. With the level of threat severity high in all of the groups, it is possible that no type of manipulation of threat or efficacy levels could persuade the participants to accept the message because the efficacy could not overcome the level of perceived threat. These results suggest that fear appeals will not make an individual more likely to accept a message advocating for increased government surveillance to fight terrorism because the level of perceived efficacy is not sufficient to overcome the threat. More broadly, Muthusamy et al. (2009) proposed that fear appeals are not effective in situations where the rate of fear is already very high. The results of this study could support such a proposition. However, proposing that fear appeals are not at all effective in high preexisting fear cases is drastic. Instead, the explanation may be that the success of a fear appeal in a high fear situation relies heavily on the level of perceived efficacy. As will be discussed below, there is evidence that perceived efficacy is the variable most likely to predict message acceptance. Thus, it is likely that if there is a preexisting high rate of fear, a successful fear appeal must have an efficacy option that is sufficient to overcome the perceived threat.

Further research is necessary to determine if the fear of terrorism in the United States is so great that it renders a fear appeal unworkable. Muthusamy et al. (2009) tested the participants'

level of fear regarding AIDS/HIV. However, in this current study, the fear variable tested the participants' general feelings of fear after reading the article, as suggested by Witte (2000). This study did not specifically ask participants how much fear they felt regarding terrorism. A future study could examine these results further by asking all participants about their fear of terrorism to better determine if a high rate of fear has an effect on the EPPM results.

This study also hypothesized that participants exposed to the government surveillance high efficacy option would have more favorable attitudes toward government surveillance than those who were not exposed to this message. However, this hypothesis was not supported. The idea behind this hypothesis was that people may generally be opposed to increased government surveillance but a high efficacy fear appeal message may persuade some people to more readily accept government surveillance to combat terrorism. It is possible that the high perceived threat of terrorism affected results. As Muthusamy et al (2009) indicated, if the fear of a topic is high, attitudes will likely not be manipulated in the way that EPPM suggests they should be.

Research suggests that the best predictors of whether a message will be accepted are response efficacy and self-efficacy (Roskos-Ewoldsen, et al, 2004; Floyd, Prentice-Dunn, & Rogers, 2000). This study found evidence to support that proposition. Response efficacy and self-efficacy combined predicted 72 percent of the variance in danger control (message acceptance), while threat severity and susceptibility combined predicated only four percent of the danger control variance. Together, threat and efficacy predicted 76 percent of the danger control variance. These results highlight the importance of efficacy within fear appeals.

Research also suggests that the level of threat is a better predictor of fear control than efficacy (Roskos-Ewoldsen, et al, 2004). The results of the current study found that threat susceptibility and severity combined predicted three percent of the variance in fear control, while

efficacy predicted .6 percent of the variance. This indicates that threat is a better predictor of message rejection than efficacy. However, both threat and efficacy predict only a small amount of the variance in message rejection, suggesting that there are other variables that can better predict whether an individual will choose the fear control process. The discussion of dissonance below offers some insight on this issue.

This study did find evidence that the type of efficacy is of consequence when drafting a fear appeal. The results indicated that the participants in the individual reporting groups were more likely to choose danger control and accept the message than those in the government surveillance efficacy groups. This suggests that the type of efficacy offered in a fear appeal needs to be taken into consideration, particularly when the audience does not find the efficacy option appealing. It also suggests that the participants were more willing to accept a message advocating for individual reporting to fight terrorism, rather than increasing government surveillance, which makes sense given the uproar over privacy concerns that took place after Snowden leaked the PRISM project information.

Overall, not all of the results are consistent with EPPM. However, the results do highlight the importance of efficacy in relation to danger control and message acceptance. The type of efficacy used and the amount of efficacy respondents perceived were key indicators as to whether the respondent would accept the message. Moreover, there is evidence that because the threat level was so high, the experimental manipulations of threat and efficacy had little impact on respondents' decision to accept or reject a message. As Muthusamy et al. (2009) suggest, this could mean that using fear appeals on groups who already have a high perception of threat or fear is ill advised. However, it may also mean that perceived efficacy is the key to fear appeal persuasion. These results suggest that influencers will need to seriously research and consider the

audience who will be receiving the fear appeal. The influencer will need to understand what efficacy options are available to the audience and how useful those options are. Most importantly, the author of a fear appeal needs to ensure that the perceived efficacy is strong enough to overcome the threat. If efficacy cannot surpass perceived threat, there is little likelihood of a successful, persuasive fear appeal.

**Privacy**

The concept of privacy was central to this study. Research suggests privacy can be conceptualized as a freedom from surveillance (Solove 2002, 2008), which was the conceptualization used in this study. Theoretically, those who are concerned about privacy should be less likely to allow increased government surveillance of phone and Internet communications. That being noted, the privacy paradox (Acquisti, 2004; Acquisti & Grossklags, 2005; Acquisti, Brandimarte & Loewenstein, 2015) is also a theory that must be considered.

Westin, Altman, Petronio, and Solove's (2008) theories suggest that privacy is about controlling access to oneself and controlling access to information about oneself (Margulis, 2011). These theories support the proposition that as privacy concern increases, attitudes toward government surveillance should decrease. It is logical that those with a high privacy concern would abhor the idea of increased government surveillance of their private communications. However, this study did not find that result. Overall, there was no significance correlation between privacy concern and attitudes toward government surveillance. To analyze this result further, the participants were divided into low and high privacy concern groups. When considering that the meaning of privacy encompasses the freedom from surveillance, it is logical that the high privacy concern group would have a much lower tolerance for government surveillance. And yet, the high privacy concern group's mean regarding attitude toward

government surveillance was practically the same as the low privacy concern's mean, which is not in line with the theories of privacy set forth by Altman, Westin, Petronio and Solove. This result could be explained two ways. The first explanation focuses on consent and control of information. When Snowden leaked information about the U.S. Government's PRISM project, U.S. citizens discovered that their personal communications may have been monitored without their knowledge or consent, which was viewed as a violation of privacy. However, if people are offered the option of allowing increased government surveillance, and knowingly choose that option, the government's access to their personal communications may not be considered a privacy violation because there was consent. This speaks to the legal concept of reasonable expectation of privacy. Often in tort and Fourth Amendment privacy violation cases, part of the determination depends on whether the individual had a reasonable expectation of privacy. If someone consents to allow government surveillance of personal communications, that person no longer has a reasonable expectation of privacy in those communications. Thus, while the government's secret monitoring of personal communication is considered a privacy violation, consenting to increased government surveillance may not be viewed as a privacy issue to some people. The second explanation involves the privacy paradox, which suggests that people are willing to give up privacy in exchange for some sort of benefit (Acquisti, 2004). In this case, the benefit could be safety and security. For example, hypothesis 2c, proposing that there would be a positive relationship between perceived threat and attitudes toward government surveillance, was supported. As the respondent's perceived threat of terrorism increased, they were more likely to be in favor of increased government surveillance. Thus, according to the results, attitudes toward government surveillance were influenced by perceived threat level and not by privacy concern. These results suggest that people are willing to give up privacy in exchange for security.

Moreover, safety may be more important to some people than keeping the government out of private communications.

The implications of these results, that respondents are more concerned about security than privacy, are troubling. The concept of privacy has grown and evolved since Warren and Brandeis' 1890 Harvard Law Review article. It is an ever-changing concept, which theorist have had a difficult time pinning down and defining. It is likely that as the threat of terrorism continues to grow, it will influence society's concerns about privacy. The danger in this can be illustrated using a freedom of speech analogy. When First Amendment lawyers discuss the regulation of speech, they often reference the "slippery slope," or the idea that, if not highly controlled and monitored, regulations on speech can snowball out of control with the result being that all speech is regulated. Privacy has its own slippery slope. The more relaxed people become about privacy and the more willing they are to allow others, including the government, to invade their privacy, the more likely that the situation could snowball out of control, with the result being no privacy for anyone. There are some people who argue that privacy is already extinct. That argument assumes, however, that privacy can be clearly defined and categorized. Research suggests this is not the case. Scholars such as Altman, Westin, Petronio, Solove and Nissenbaum have been clear that privacy is difficult to define and has different meanings to different people. The argument that privacy is extinct also does not take into account Fourth Amendment privacy. In 2014, the Supreme Court decided that individuals have a reasonable expectation of privacy in the information contained on their cell phones (*Riley v. California*). At least in the sense of the Fourth Amendment, there is still an argument that privacy exists. Society's reaction to Snowden's leak of the PRISM project also suggests that privacy is a right that is highly valued in our society, yet it is a concept that must evolve with technology. Changes in society's

understanding of privacy is not necessarily a bad thing. However, giving up privacy can lead to dire consequences. Once privacy is relinquished, it is not something that can easily be regained later.

Another hypothesis was that privacy concern and fear control (message rejection) would be correlated. In this study, there were two efficacy messages: 1) increased government surveillance can work to combat terrorism and 2) individual reporting of suspicious activity can help to fight terrorism. If the participants gravitated toward the danger control process, then they were accepting the fear appeal message. However, if they gravitated toward the fear control process, they were effectively rejecting the fear appeal message. When looking specifically at the government surveillance message groups, there was no significant correlation between privacy concern and message rejection. However, when isolating the individual reporting groups, there was a significant positive correlation between privacy concern and fear control. The correlation was weak, but it indicated that as privacy concern increases the tendency to reject the message increases. In other words, as the participant's privacy concern increases, the participant will be more likely to reject the message that reporting suspicious activity to authorities can combat terrorism.

This result then led to the following question: If participants with increased privacy concerns are more likely to *reject* the message that individual reporting of suspicious activities helps to fight terrorism, does that mean that participants with increased privacy concerns will be less likely to intend to report suspicious activity to authorities? In this case, the answer to that question was in the negative. The results suggested that as the level of privacy concern increases, the likelihood that the participant will report suspicious activity also increases. It may initially appear that these two results conflict with each other. On the one hand, as privacy concern

increases, the participant is more likely to reject the message that individual reporting of suspicious activity can help fight terrorism, on the other hand, as privacy concern increases, the participant is more likely to intend to report suspicious activity to authorities. However, as is clarified below, these results can be explained using conceptualizations of privacy and the privacy paradox.

The broad understanding of privacy boundary building indicates that as privacy concern increases, the individual will be less likely to want to open an avenue of communication between herself and government authorities. For example, Altman's (1976) theory of privacy, which continues to be widely cited today, suggests that privacy can be conceptualized as the "selective control of access to the self or to one's group" (Altman, 1976, p. 8; Altman, 1977; Marguilis, 2011). According to Altman (1976), this conceptualization allows for certain properties that can help further the understanding of privacy. First, privacy can be viewed using several different social units (such as individuals or groups). Second, privacy is recognized as a "bidirectional" process, meaning that information can flow *from* the individual or *to* the individual (Altman, 1976, p. 8). Third, the control of information is a selective and dynamic process that can continually change. Altman (1976) viewed access to self is a "dynamic regulatory process" (p. 8). His theory suggests a dialectical tension between opening an avenue to share information with others and closing that avenue. Altman viewed self-disclosure as openness and privacy as closedness, which he believed were two separate processes that could be woven into a dialectic model (Petronio, 2002). Petronio's communication privacy management (CPM) theory builds off Altman's dialectical approach and proposes that self-disclosure and privacy are inseparable features of a more defined and consolidated dialectic process (Margulis, 2011; Petronio, 2002). Petronio (2002) views privacy as a constant battle that every person contends with every single

day. Any disclosure that we make needs to be weighed through the dialectic give and take process (Petronio, 2002). Regarding privacy, Petronio (2002) states:

> We are constantly in a balancing act. We try to weigh the demands of the situation with our needs and those of others around us. It gives us a sense that we are the rightful owners of information about us. There are risks that include making private disclosures to the wrong people, disclosing at a bad time, telling too much about ourselves, or compromising others. (p.1)

Under this conceptualization of privacy, each person has built a metaphorical boundary around herself/himself that is flexible and adaptable. During the course of each day, the person is making decisions about whether to let information pass through that boundary. If a person loses control of certain aspects of that boundary there can be turbulence, which could lead to a violation of privacy (Petronio, 2002).

The boundary building conceptualization of privacy helps to explain why the increase in privacy concern is related to an increase in fear control. The individual reporting efficacy message used in the experiment sought to persuade participants that contacting authorities to report suspicious activity is effective in combating terrorism. Rejecting this message means pushing back on the idea that opening a line of communication with the government can work to fight terrorism. Theoretically, the more an individual is concerned about privacy the more likely the individual will be to reject a message that advocates for opening a line of communication with government authorities. Thus, privacy concern should have a positive relationship with message rejection (fear control), which it did here. Contacting police usually means having to provide information such as name, phone number, address and current location. It could also open an avenue for the police to contact the individual at a late time to gather more information. Clearly, reporting suspicious activity to authorities is likely to lead to the release of private information. If the individual opens that line of communication and then loses control of that

boundary, then the resulting turbulence could lead to a violation of the privacy principles. Petronio (2002) suggests that people want to keep control of their boundaries. A choice to reject the idea that contacting authorities can fight terrorism is a choice to maintain control of privacy boundaries.

At the same time, the results also found that as privacy concerns increased, the intention to report suspicious activity to police also increased. Considering the theories of privacy and boundary building, the relationship between privacy concern and intentions to contact authorities should be negative. It may seem obvious that if an individual sees something suspicious that person should call the police. However, that reasoning fails to consider the conceptualizations of privacy. Scholars (Altman, 1976; Petronio, 2002; and Westin, 2003) make it clear that every decision we make regarding communicating information to another person must involve a decision about privacy. A positive correlation between privacy concerns and an intent to contact authorities seems to be in contention with the understanding of privacy. The privacy paradox, however, offers an explanation for this phenomenon. The privacy paradox suggests that people are willing to give up privacy in exchange for a benefit. In this case, the benefit is safety and security. This would explain why people with a high level of privacy concern would be willing to open a communication boundary to report suspicious activity to the police. Nissenbaum's (2004) theory of contextual integrity offers another possible explanation. Contextual integrity looks specifically at the flow of information from one person to another. It suggests that decisions regarding the sharing of private information are made based on the context surrounding the sharing of information and content of the information being shared. As long as the individual feels that the correct information is shared in the correct context, there will be no breakdown of contextual integrity and no privacy violation. In this case, it could be that people with a higher

privacy concern do not view contacting the police to report suspicious activity as a privacy issue because the information matches up with the context in which the information is being shared. Normally, a privacy-minded individual may not willingly open an avenue with the government in which the person must provide personal information such as name, phone number, address and current location. However, if the person believes that sharing that private information with the government makes sense in the context of reporting a possible crime, there may be no breakdown of contextual integrity and no privacy violation. In other words, it makes contextual sense to contact the police and tell them who and where you are when reporting suspicious activity, so there would be no privacy violation. Future research regarding privacy concerns and the intent to open an avenue of communication with the government would help to further explain these results and how people understand the concept of privacy.

It is also likely that increased fear about the loss of security has an effect on privacy concerns. Altman recognized that after the terror attacks of 2001, making sense of privacy has become more muddled. In the Foreword to Petronio's book, *Boundaries of Privacy,* Altman states that the attack left us "unsure about how to cope with the immediate and long-term specter of terrorism" (Petronio, 2002, p. xiii). Furthermore, he contended that society will face new privacy challenges in the twenty-first century as technology evolves and our personal information becomes more accessible to others. The literature review section of this study notes that combating terrorism and privacy go hand-in-hand. As illustrated in case law (*i.e., Berger v. New York)* and statutory law (*i.e.*, FISA), in the fight against terrorism, the government relies heavily on the interception of private communications. Thus, it is inevitable that a discussion about national security must involve privacy. It is also quite probable that the terror attacks of 2001 have altered society's understanding of privacy. Although scholars like Petronio (2002)

suggest that privacy is important to people, there is also a willingness to open lines of communication with the government in an effort to obtain security.

Research regarding privacy issues is important to a variety of groups. For example, understanding society's privacy concerns is important to legislators who write statutory laws dealing with national security and privacy, to civil rights attorneys and organizations who argue in favor of increased privacy, and to judges who must decide whether a privacy right has been violated. The concept of privacy constantly changes and evolves. Moreover, it is highly subjective. Scholars agree that it is difficult to offer one robust conceptualization of privacy (Acquisti, 2004; Acquisti & Grossklags, 2005; Acquisit et al., 2015; Altman, 1976; Gormley, 1992; Nissenbaum, 2004; Prosser, 1960; Solove, 2002; and Westin, 2003). Scholars also agree that understanding privacy is important to society (Altman, 1976; Nissenbaum, 2004; Solove, 2002; and Westin, 2003) and as technology and communication change, further research regarding privacy is necessary (Petronio, 2002). The results of this study indicate that people may be willing to give up privacy rights in exchange for security and that attitudes about government surveillance are influence more by the threat of terrorism than by privacy concerns. This information is important to people who are trying protect privacy in the United States and illustrates that the fear of terrorism may negate privacy concerns.

**Cognitive Dissonance**

Another purpose for this study was to investigate whether cognitive dissonance, more specifically the level of dissonance felt while reading a fear appeal, is related to the EPPM variables and whether dissonance can predict message acceptance or rejection. As hypothesized, dissonance was related to the individual EPPM variables. Dissonance had statistically significant relationships with fear, perceived response efficacy and perceived self-efficacy. Unexpectedly,

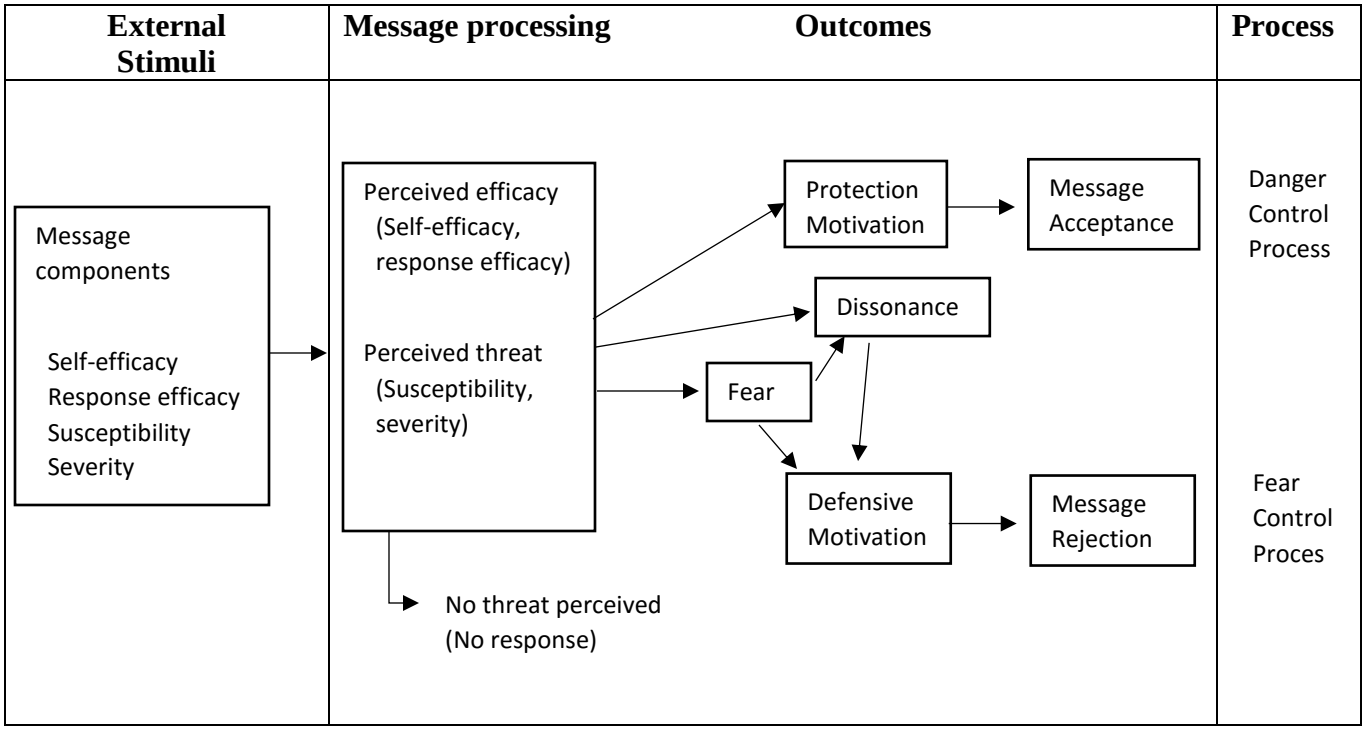
there was no correlation between dissonance and perceived threat susceptibility and severity, suggesting that reading about a threating topic does not, on its own, lead to an increase in dissonance. The rest of the results were as expected. As fear increased, dissonance also increased, and those who had a lower perception of self and response efficacy had a greater feeling of dissonance. It is logical that an individual will feel dissonance when reading a message suggesting that the person has little or no efficacy to combat a threat. Moreover, research suggests dissonance can "arise from exposure to an attitude-challenging news source or information" (Metzger et al, 2015, p. 5). This study found further evidence of this proposition. The hypothesis that, when isolating the government surveillance efficacy group, dissonance increased as attitudes toward government surveillance decreased, was supported. In other words, when participants who had negative attitudes regarding government surveillance read an article about increased government surveillance, they were more likely to feel dissonance. This is in line with the proposition that reading information challenging personal beliefs will lead to mental discomfort (Metzger et al, 2015).

The results indicated that dissonance was minimally related to message acceptance. As other scholars have suggested, perceived efficacy explained more of the variance in danger control than perceived threat (Roskos-Ewoldsen, et al, 2004; Floyd, Prentice-Dunn, & Rogers, 2000). Here, efficacy explained 71 percent of the danger control variance, while threat explain three percent of the variance. Dissonance explained only .3 percent of the danger control variance. Perceived response efficacy and self-efficacy mediated the influence of dissonance on danger control. Taken together, fear, threat and efficacy explained 76 percent of the danger control variance, and dissonance did little to increase that percentage.

This study found a strong relationship between dissonance and fear control. As dissonance increased, the participant was more likely to reject the fear appeal message. In addition, two of the EPPM's variables, perceived threat severity and response efficacy mediated the influence of dissonance on fear control. Interestingly, the results indicated that dissonance was a better predictor of fear control than the other EPPM variables. As noted previously, research suggests that perceived threat is a better predictor of fear control than efficacy (Roskos-Ewoldsen, et al, 2004). The results of this study suggest that is true, but also that dissonance is a better predictor of fear control than perceived threat. Perceived threat predicted only seven percent of the variance in fear control, while, when controlling for the other variables, dissonance predicted 30 percent of the variance. This finding illustrates that a feeling of mental discomfort could lead a person to more readily reject a fear appeal message. These results suggest that dissonance is an important variable when investigating and predicting fear control. It must be noted that all of the EPPM variables and dissonance combined explained only 37 percent of the fear control variance, which suggests that additional variables or group of variables may help to better predict fear control.

Clearly, dissonance is an important factor when attempting to persuade using fear appeals, especially in regard to message rejection. Dissonance did play a role in motivating participants to choose the fear control route. Witte et al. (1998) suggests that fear is a strong motivator and that when people perceive a serious threat, people will be desperate to take some sort of action to reduce their fear. In addition, the level of efficacy determines whether that person gravitates to danger control or fear control (Witte et al. 1998). The results of this study further suggest that dissonance plays a role in whether someone is motivated to choose the fear control route. Thus, a better EPPM model may be the following:

**Figure 8. The extended parallel process model (Maloney et al., 2011)**




Like EPPM, the above theoretical model suggests that perceived threat and perceived efficacy continue to have the primary influence on whether a person is motivated toward the danger control process, and fear still leads to fear control. However, dissonance has been inserted as a new variable that may also lead to the fear control process. The results suggested that dissonance was a much better predictor of message rejection than fear. Under this model, it is possible that fear could lead to dissonance, which would then lead to defensive motivation, or dissonance can motivate a person to head directly to defensive motivation, bypassing fear.

These results speak to what factors lead to a successful persuasive message. If the author of the fear appeal wants the reader to be motivated to choose the danger control route and not fear control, then dissonance needs to be taken into consideration. This may be particularly important when dealing with issues where there is already a preexisting, heightened level of threat or fear. For example, efficacy is more likely to predict the danger control process (Roskos-

Ewoldsen, et al, 2004; Floyd, Prentice-Dunn, & Rogers, 2000). However, when dealing with issues that cause a preexisting high amount of fear, the efficacy content in a message has little to no impact on the danger control process. In that type of situation, dissonance may play a key role in whether a fear appeal is effective.

However, even in other instances, dissonance needs to be considered when formulating a fear appeal. Research suggests that the "management" of dissonance can be particularly important when trying to reach audiences (Westerwick et al., 2013, p 445). According to Westerwick et al. (2013), "if users anticipate viewing attitude-challenging content, they may first bolster their pre-existing attitudes and then explore other perspectives" (p. 445). A bolstering of pre-existing attitudes could have an effect on persuasion. Another issue to consider is that it is not just the substantive information in the fear appeal that could lead to dissonance. Dissonance can result from a dislike or distrust of the source of the message (Metzger et al. 2015). Thus, when drafting a fear appeal, the author needs to consider the primary audience the message is attempting to persuade. The source of the fear appeal and how it is worded should be carefully formulated to appeal to the specific audience because cognitive dissonance could result in rejection of the message.

These results speak to the broad future use of EPPM. The theory is widely used in health communication, where persuasion is often viewed in a positive light. For example, persuasive messages can help keep people safe by advocating for the use of condoms, vaccines and making healthy choices. The results in this study are not, however, advocating for persuasion to be used to convince people to give up privacy rights. Rather, this study investigated whether fear appeals work the same way in a privacy situation as they do in a health communication situation. Finding that the fear appeals in this study did not lead to message acceptance is not an unsatisfactory

result. It could be that people view the efficacy options in health communication (*i.e.* putting on a condom) as a different sort of choice than giving up privacy rights. For privacy advocates, the more concerning finding is that individuals care more about security than privacy. The results of this study suggest that the danger may not be that people can be persuaded to give up privacy rights, but rather, that people will make that choice on their own in exchange for safety.

*Dissonance, Privacy Concern and the Privacy Paradox*

This study proposed that there would be a relationship between privacy concern and cognitive dissonance. In addition, post hoc analyses examined the relationship between cognitive dissonance and the privacy paradox.

There was no support for the hypothesis that, when looking only at the government surveillance efficacy groups, there would be a positive relationship between privacy concern and dissonance. The theoretical foundation for this hypothesis combined the theory of cognitive dissonance and a conceptualization of privacy (*i.e.* freedom from surveillance) (Solove, 2002). It is logical that if someone with a high privacy concern reads an article about increased government surveillance, that person would feel dissonance. The lack of support for this hypothesis could be because it was an analysis of a subgroup of the sample. Because all the experimental stimulus articles pertained to some sort of government interaction and communication with individuals, either through contacting the authorities or allowing increased government surveillance, a post hoc analysis was conducted on the entire experimental sample to examine the relationship between dissonance and privacy concern. The results showed a weak positive relationship, suggesting that as concerns about privacy increased, dissonance also increased. This finding is in line with the theoretical foundation created by combining privacy and dissonance theories. It offers support for the proposition that dissonance can occur when a

person is exposed to belief-challenging information. In other words, as an individual becomes more concerned about protecting private information and less welcoming to opening a line of communication with the government, that individual will feel dissonance when reading an article about sharing private information with the government to help fight terrorism. As previously explained, dissonance plays a role in whether someone is motivated toward fear control. Thus, if a fear appeal is to be successful, the relationship between dissonance and reading belief-challenging information needs to be considered.

A final post-hoc hypothesis focused on the privacy paradox and its relationship to dissonance. The hypothesis, which was supported, proposed that privacy concerns and intentions to allow government surveillance would predict dissonance. Cognitive dissonance, an inconsistency between attitudes and intentions or behaviors, and the privacy paradox, an inconsistency between attitudes toward privacy and intentions or behaviors regarding privacy, are likely related. Theoretically, it is probable that people who display a privacy paradox also feel cognitive dissonance. For example, if a person with a high privacy concern intended to allow increased government surveillance, that person should feel dissonance because of the discrepancy between attitude and intentions. The results of this study support that proposition.

These results lead to the question: How do people who exhibit a privacy paradox find consistency? Festinger (1957) suggests that when individuals feel dissonance, they will try to alleviate that dissonance in some fashion, likely by changing either their attitudes or behaviors. The privacy paradox is an inconsistency that has been clearly documented (Acquisti, 2004; Acquisti & Grossklags, 2005; Acquisti, Brandimarte & Loewenstein, 2015), and it appears to be persistent. Festinger (1957) recognizes that some types of dissonance may never end, resulting in a constant struggle for some sort of consistency. The privacy paradox could be one of those types

of inconsistencies. Perhaps people recognize the inconstancy and are constantly striving to resolve the discrepancy. Another explanation could be that people use psychological distortions such as hyperbolic discounting and immediate gratification (Aquisti, 2004) to trick their minds into believing that there is no inconsistency. For example, people may discount the future cost or risk of sharing private information, or they may deem the benefit of sharing the information more rewarding than the cost. These types of psychological distortions help to explain the privacy paradox and could offer individuals a resolution to dissonance, even if the resolution is illusory. It could also be that the inconsistency is never resolved because people are unable to recognize that their behaviors and attitudes regarding privacy are conflicting. Aquisti (2004) states:

> Whenever we face privacy sensitive decisions, we hardly have all data necessary for an informed choice. But even if we had, we would be likely unable to process it. And even if we could process it, we may still end behaving against our own better judgment. (24)

If no inconsistency is detected, dissonance may not be recognized for what it is, and there would be no effort to reach resolution. A more concerning answer is that a person who exhibits a privacy paradox many eventually resolve the inconsistency by changing his or her attitude toward privacy, and perhaps, become willing to give privacy up. Finally, it must be considered that privacy means different things to different people. Altman and Petronio (2002) both recognized that technology has an effect on privacy concerns. As technology evolves, privacy does as well, and each person's privacy needs are different. It could be that the privacy paradox is the result of trying to place everyone into a privacy box in which some people simply do not fit. Future research focusing on dissonance and the resolution of the inconsistency created by the privacy paradox would help provide a full explanation to this issue.

What the results of this study make clear is that concerns about privacy and the intent to allow government surveillance can predict dissonance, which suggests that dissonance and the privacy paradox are related. Future research is necessary to further investigate this relationship. It is possible that the privacy paradox is an example of dissonance. If that is the case, then the issue of how the inconsistency is resolved is an important question that needs to be answered. The most concerning explanation would be that people resolve the inconsistency by simply letting go of their privacy beliefs, which could eventually lead to the extinction of privacy rights. Future research focusing on the privacy paradox and dissonance should provide further explanations. Understanding the privacy paradox can help us to understand why people make decisions about sharing private information and if/why people are willing to give up privacy for security. Answers to these questions are important to businesses and advertisers that want people to share private information for a benefit, but these answers are also critical to legislators who make privacy laws, attorneys who argue for privacy rights, and judges who make legal privacy decisions.

**Limitations and threats to validity**

There were some limitations to this study. Although research indicates that online samples are diverse and good quality (Buhrmester et al., 2011), they are not generalizable to the general public. Further, although Qualtrics assured the researcher that a general population random sample would be close to equal parts men and women, that was not the case in this study. Nearly 80 percent of the participants were women. In addition, most of the participants were white. Controlling for race and gender showed no significance between the groups. However, a more diverse sample would have been preferred because diversity in samples is considered a desirable trait in quantitative research (Buhrmester et al., 2011).

Because this study uses experimental methods, there were some threats to validity. The experiment ran from January 13, 2007 to January 19, 2007. A week before the experiment ran, on January 6, a gunman opened fire at a Florida airport, killing five people. Because this event happened near the time of the experiment, it is possible that the perceived threat level pertaining to terrorism was higher than it might normally be. Furthermore, it is possible that the perceived threat of terrorism is always high in today's society. Research suggests that when a pre-existing threat exists, fear appeals may not be effective (Muthusamy et al, 2009). With the perceived threat so high, it is difficult to determine if any type of fear appeal could be effective. In addition, this study did not ask the respondents about their fear of terrorism. Future research is necessary to determine how high the fear of terrorism is in the United States and how that fear affects the persuasiveness of fear appeals.

## Chapter 7: Conclusion and future research

This study explained the linkage between privacy, government surveillance and national security. Scholars offer several conceptualizations for privacy (Altman, 1976; Nissenbaum, 2004; Solove, 2002; and Westin, 2003), and one of those is being free from surveillance. This study used that conceptualization of privacy in its analysis. U.S. citizens have a constitutional right to be free from warrantless searches by the government. When overbroad surveillance techniques pick up the online conversations of people who are not under investigation, that privacy right is violated. The reasons set forth by the government for conducting surveillance of communications is for the protection of national security. The connection of these concepts helped to drive the experimental portion of this study.

This study also sought to investigate privacy through a series of analyses, which included testing whether a fear appeal can persuade respondents to feel favorably toward increased government surveillance using the Extended Parallel Process Model (EPPM), investigating the relationship between privacy concerns and attitudes toward increased government surveillance, and examining the privacy paradox and how it is related to dissonance. In addition, this study tested whether dissonance is related to fear appeals and persuasion.

EPPM proposes that fear appeals can be used as a persuasive technique to motivate the reader of the message to take a certain action that will benefit the reader in some way. The theory tends to be used in the study of health communication to promote positive and healthy habits. This study tested EPPM outside of the health communication context to examine if fear appeals can persuade people to give up privacy rights in exchange for better security. The results suggest that the threat of terrorism was too high for a fear appeal to have a persuasive effect on people's attitudes and intentions. This finding offers further evidence that, for a fear appeal to be

effective, the level of perceived efficacy must overcome the level of perceived threat. The results also offer evidence that fear appeals may be ineffective when pre-existing threat levels are high. Further research about the level of fear regarding terrorism in the United States can help to determine whether a pre-existing fear is disturbing the effectiveness of the fear appeals. This study also found evidence that cognitive dissonance is related to the EPPM variables. Dissonance is a better predictor of message rejection than fear, threat and efficacy combined. Because of the predictive power of dissonance, it is a variable that should be included in the EPPM model. This is particularly important when a higher perception of threat already exists. The results also indicated that efficacy is the best predictor of danger control. These results are evidence of the importance of efficacy in a fear appeal. Those who are seeking to influence with fear appeals need to investigate the threat level of an issue and how severe the threat is to the readers of the fear appeal. The influencer then needs to consider the efficacy options available to the readers. Only those efficacy options that are strong enough to overcome the perceived threat level will provide for an effective fear appeal. The influencer must also consider the readers' feelings toward the efficacy options, because if the readers feel dissonance when exposed to the fear appeal, they may be more likely to navigate toward fear control. These are important considerations that can help advance the effectiveness of fear appeals, particularly in the field of healthcare where the acceptance of efficacy options such as condom use can prevent the spread of contagious diseases.

Although research suggests that fear appeals are useful in the field of healthcare, there is also danger in using fear as a persuasive tool. A focus of this study was to discover whether fear appeals could be used to persuade people to give up privacy rights and allow increased government surveillance. This study did not find support for that hypothesis, but the results

suggest that if the efficacy is manipulated in a way that enables the audience's efficacy level to surpass the high threat level, persuasion will likely take place. In other words, if the level of efficacy people feel regarding increased government surveillance is raised so that it surpasses the threat of terrorism, there is a likelihood that people can be persuaded to give up their privacy rights. For privacy advocates, this is concerning news because it means that people may be persuaded to give up privacy rights if a fear appeal is sufficiently manipulated.

Surprisingly, this study did not find a relationship between privacy concern and attitudes toward government surveillance. Attitudes toward government surveillance were the same no matter if the respondent had a high or low privacy concern. Overall, attitudes toward government surveillance were neutral, with a mean of 4.41 out of seven. Importantly, there was a relationship between perceived threat and attitudes toward government surveillance. The study found that as the threat of terrorism increased, attitudes toward government surveillance became more favorable. Taken together, these results suggest that perceived threat, and not privacy concern, influenced attitudes toward government surveillance. This is important information for constitutional lawyers. The legal test used to prove the government has invaded a person's Fourth Amendment right to privacy is: an actual expectation of privacy that society would consider reasonable. The effectiveness of this argument depends on what society recognizes as a reasonable expectation of privacy. If society begins to favor security over privacy, constitutional attorneys could encounter serious problems with meeting the legal standard for Fourth Amendment privacy. In other words, if society begins to believe that in order to keep people secure the government should be able to monitor private communications, then according to the Fourth Amendment privacy legal standard, society would no longer recognize a reasonable expectation of privacy in personal communications. This would open an avenue for the

government to monitor private communications without having to overcome the Fourth Amendment hurdle. Because of advancements in technology, society's expectations of privacy continue to evolve. There is evidence that after the terror attacks of 2001, understandings regarding privacy have become muddled as people strive for security (Petronio, 2002). It is critical for constitutional lawyers to keep abreast of changes in privacy concerns and understand how privacy is perceived by society today.

In addition, this study found that the privacy paradox can help to explain why respondents with a high privacy concern had nearly the same attitudes toward government surveillance as respondents with low privacy concerns. The privacy paradox suggests that people are willing to give up privacy in exchange for a benefit. In this case, there is evidence that respondents with a high level of privacy concern are willing to give up that privacy in favor of security. These results are again significant for constitutional lawyers because they indicate that people are willing to relax their expectations of privacy in exchange for security, which could suggest a shift in society's reasonable expectation of privacy. Future research into terrorism and privacy could help to further determine the effects of the privacy paradox.

It is also clear that the privacy paradox and cognitive dissonance are related. It is likely that people who display a privacy paradox encounter cognitive dissonance. The theory of cognitive dissonance suggests that, to alleviate an inconsistency, a person will either change their beliefs or their actions. An analysis of dissonance and the privacy paradox together would suggest that people who encounter a privacy paradox are constantly struggling for consistency, and at some point, will likely change their beliefs or attitudes. This could mean that as people seek security, they will be more willing to change their beliefs that privacy is important. Future

research involving dissonance and the privacy paradox could help to explain how or if the inconsistency is resolved.

Finally, more research needs to be conducted to truly understand what privacy means to society. It is not clear that privacy means the same thing to every person. As such, the privacy paradox could be the result of trying to place people into privacy categories where they do not fit. Future research that delves deeper into how people feel about privacy and government surveillance could offer a more in-depth explanation. Understanding what privacy means to society is important for attorneys, lawyers, judges, legislators and scholars. It can be critical in proposing new national security legislation and making legal arguments about Fourth Amendment privacy.

# Appendices

## Appendix A: Measures

Each participant was asked 80 questions: 6 items for threat; 14 for efficacy; 6 for fear; 9 for cognitive dissonance; 10 for attitudes toward government surveillance/individual reporting; 3 for future intentions; 11 for fear control; 8 for privacy concern; 6 for attitudes toward the U.S. government; 1 for cyber-theft and 6 for demographics.

1) Items for Perceived Threat Susceptibility

| To what extent do you agree with the following statements? | 1 (strongly disagree) to 7 (strongly agree) |
|---|---|
| It is likely that I will be affected by terrorism. | 1 2 3 4 5 6 7 |
| It is possible that I will be affected by terrorism. | 1 2 3 4 5 6 7 |
| I am at risk of being a victim of terrorism. | 1 2 3 4 5 6 7 |
| I am at risk of being affected by terrorism | 1 2 3 4 5 6 7 |

2) Items for Perceived Threat Severity

| To what extent do you agree with the following statements? | 1 (strongly disagree) to 7 (strongly agree) |
|---|---|
| I believe the risk of terrorism is serious. | 1 2 3 4 5 6 7 |
| I believe the risk of terrorism is significant. | 1 2 3 4 5 6 7 |
| I believe the risk of terrorism is severe. | 1 2 3 4 5 6 7 |

3) Items for Perceived Self-Efficacy (Broken down by efficacy option)

a. Government surveillance

| To what extent do you agree with the following statements? | 1 (strongly disagree) to 7 (strongly agree) |
|---|---|

| | |
|---|---|
| I am able to allow increased government surveillance in order to prevent terrorism. | 1 2 3 4 5 6 7 |
| Allowing increased governmental surveillance is easy to do in order to prevent terrorism. | 1 2 3 4 5 6 7 |
| Allowing increased governmental surveillance to prevent terrorism is convenient. | 1 2 3 4 5 6 7 |

b. Individual reporting

| To what extent do you agree with the following statements? | 1 (strongly disagree) to 7 (strongly agree) |
|---|---|
| I am able to report suspicious activities to law enforcement in order to prevent terrorism | 1 2 3 4 5 6 7 |
| Reporting suspicious activity to law enforcement is easy to do in order to prevent terrorism | 1 2 3 4 5 6 7 |
| Reporting suspicious activity to law enforcement to prevent terrorism is convenient. | 1 2 3 4 5 6 7 |

4) Items for Perceived Response Efficacy (Broken down by efficacy option)

a. Government surveillance

| To what extent do you agree with the following statements? | 1 (strongly disagree) to 7 (strongly agree) |
|---|---|
| Governmental surveillance works to prevent terrorism. | 1 2 3 4 5 6 7 |
| Governmental surveillance is effective in preventing terrorism. | 1 2 3 4 5 6 7 |
| If I allow increased governmental surveillance, I am less likely to be affected by terrorism. | 1 2 3 4 5 6 7 |
| Increased governmental surveillance, is important to combat the threat of terrorism. | 1 2 3 4 5 6 7 |

b. Individual reporting

| To what extent do you agree with the following statements? | 1 (strongly disagree) to 7 (strongly agree) |
|---|---|
| Individual reporting of suspicious activity to law enforcement works to prevent terrorism. | 1 2 3 4 5 6 7 |
| Individual reporting of suspicious activity to law enforcement is effective in preventing terrorism. | 1 2 3 4 5 6 7 |

| | |
|---|---|
| If I report suspicious activity to law enforcement, I am less likely to be affected by terrorism. | 1 2 3 4 5 6 7 |
| Individual reporting of suspicious activity is important to combat the threat of terrorism. | 1 2 3 4 5 6 7 |

## 5) Items for Fear

| How did this article make you feel about terrorism? | 1 (not at all) to 7 (very much) |
|---|---|
| Frightened | 1 2 3 4 5 6 7 |
| Tense | 1 2 3 4 5 6 7 |
| Nervous | 1 2 3 4 5 6 7 |
| Scared | 1 2 3 4 5 6 7 |
| Anxious | 1 2 3 4 5 6 7 |
| Uncomfortable | 1 2 3 4 5 6 7 |

## 6) Items for Cognitive Dissonance

| To what extent do you agree with the following statements? | 1 (strongly disagree) to 7 (strongly agree) |
|---|---|
| I regret reading this news story. | 1 2 3 4 5 6 7 |
| I disliked reading this news story because it challenged my beliefs. | 1 2 3 4 5 6 7 |
| I agree with the stance taken in this article (reverse coded) | 1 2 3 4 5 6 7 |
| I felt uncomfortable while reading this news story. | 1 2 3 4 5 6 7 |
| This story made me question my own beliefs about terrorism. | 1 2 3 4 5 6 7 |
| I enjoyed reading this news story (reverse coded). | 1 2 3 4 5 6 7 |
| The topic of the article made me feel uncomfortable. | 1 2 3 4 5 6 7 |
| I liked the topic of this article. (reverse coded) | 1 2 3 4 5 6 7 |

| | |
|---|---|
| This story made me question my own beliefs about governmental surveillance. | 1 2 3 4 5 6 7 |
| This story made me question my own beliefs about individual reporting | 1 2 3 4 5 6 7 |

7) Items for Danger control (Broken down by efficacy option)

a. Attitudes

i.) Governmental Surveillance

| Please rate your attitude toward increasing governmental surveillance in order to combat terrorism | | | | | | | |
|---|---|---|---|---|---|---|---|
| Bad | O | O | O | O | O | O | O Good |
| Undesirable | O | O | O | O | O | O | O Desirable |
| Unfavorable | O | O | O | O | O | O | O Favorable |
| Not effective | O | O | O | O | O | O | O Effective |
| Not useful | O | O | O | O | O | O | O Useful |
| Disapprove | O | O | O | O | O | O | O Approve |

ii.) Individual Reporting

| Please rate your attitude toward individual reporting of suspicious activity to law enforcement to combat terrorism | | | | | | | |
|---|---|---|---|---|---|---|---|
| Bad | O | O | O | O | O | O | O Good |
| Undesirable | O | O | O | O | O | O | O Desirable |
| Unfavorable | O | O | O | O | O | O | O Favorable |
| Not effective | O | O | O | O | O | O | O Effective |
| Not useful | O | O | O | O | O | O | O Useful |
| Disapprove | O | O | O | O | O | O | O Approve |

b. Intentions

i.) Governmental Surveillance

| To what extent do you agree with the following statement? | 1 (strongly disagree) to 7 (strongly agree) |
|---|---|
| I would consent to increased government surveillance in order to help prevent terrorism. | 1 2 3 4 5 6 7 |
| I would contact my state and federal legislators about increasing government surveillance in order to help prevent terrorism. | 1 2 3 4 5 6 7 |
| I would allow increased government surveillance in order to combat terrorism. | 1 2 3 4 5 6 7 |

ii.) Individual Reporting

| To what extent do you agree with the following statement? | 1 (strongly disagree) to 7 (strongly agree) |
|---|---|
| I intend to report suspicious activity to law enforcement in order to help prevent terrorism. | 1 2 3 4 5 6 7 |

8) Items for fear control

a. Defensive avoidance

| Please answer the following questions. | |
|---|---|
| When I first heard about terrorism, my initial instinct was to [not want to/want to] think about terrorism | a. Not want<br>b. Want to |
| When I first heard about terrorism, my initial instinct was to [not want to/want to] do something to protect myself from terrorism | a. Not want<br>b. Want to |

b. Message minimization

| Please rate the following adjectives about terrorism. The issue of terrorism is: | 1 (Strongly disagree) to 7 (Strongly agree) |
|---|---|
| Distorted | 1 2 3 4 5 6 7 |

| | |
|---|---|
| Overblown | 1 2 3 4 5 6 7 |
| Exaggerated | 1 2 3 4 5 6 7 |
| Boring | 1 2 3 4 5 6 7 |
| Overstated | 1 2 3 4 5 6 7 |

## c. Perceived manipulation

| Please rate how you felt about the article. The article was: | 1 (Strongly disagree) to 7 (Strongly agree) |
|---|---|
| Manipulative | 1 2 3 4 5 6 7 |
| Misleading | 1 2 3 4 5 6 7 |
| Exploitative | 1 2 3 4 5 6 7 |
| Distorted | 1 2 3 4 5 6 7 |

## 9) Items for privacy concern

| Please respond to the following questions. | 1 (not at all) to 7 (very much) |
|---|---|
| In general, how concerned are you about your privacy while you are using the Internet? | 1 2 3 4 5 6 7 |
| In general, how concerned are you about your privacy while talking on your phone or cellphone? | 1 2 3 4 5 6 7 |
| Are you concerned about people online not being who they say they are? | 1 2 3 4 5 6 7 |
| Are you concerned about people you do not know obtaining personal information about you from your online activities? | 1 2 3 4 5 6 7 |
| Are you concerned that an email you send may be read by someone else besides the person you sent it to? | 1 2 3 4 5 6 7 |
| Are you concerned that you are asked for too much personal information when you register or make online purchases? | 1 2 3 4 5 6 7 |
| Are you concerned about online identity theft? | 1 2 3 4 5 6 7 |
| Are you concerned who might access your financial records electronically? | 1 2 3 4 5 6 7 |

11) Attitudes toward the U.S. Government

| Please rate your attitude toward the U.S. Government | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Bad | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Good |
| Untrustworthy | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Trustworthy |
| Dishonest | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Honest |
| Unfavorable | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Favorable |
| Not effective | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Effective |
| Not useful | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Useful |
| Disapprove | ○ | ○ | ○ | ○ | ○ | ○ | ○ | Approve |

12) Cyber-theft

Have you ever been the victim of cyber-theft or identity theft? Yes____ No_____

Do you know anyone who has been the victim of cyber-theft or identity theft? Yes_____ No____

13) What does Privacy mean to you? _____

14) Items for Demographics

| | |
|---|---|
| What is your age? | _____ (Please write in age) |
| What is your gender? | Male<br>Female<br>Other |
| Please specify your ethnicity/race. | African American<br>Native American<br>Caucasian<br>Asian/Pacific Islander<br>Other |
| Are you Hispanic/Latino? | Yes<br>No |
| What is the highest level of education you have completed? | Some high school, no diploma<br>High school graduate, diploma or the equivalent<br>Some college credit, no degree<br>Trade/technical/vocational training<br>Associate degree<br>Bachelor's degree<br>Master's degree<br>Professional degree<br>Doctorate degree |

| | |
|---|---|
| What is your political affiliation? | Democrat<br>Republican<br>Independent<br>Other _____ (please write in affiliation) |

## Appendix B: Fear appeal message

The following are the eight stimuli were used in the experiment. In each stimulus, the threat/efficacy were manipulated. The base article for the stimuli was taking from a CNN article. The efficacy portions were manipulated using various online sources that are referenced at the end of this appendix.

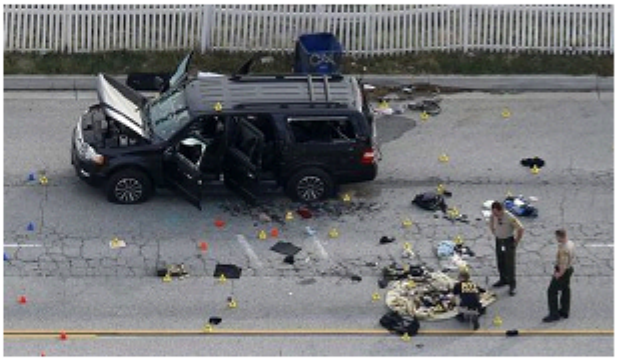
CNN

# Top U.S. intel official: ISIS can stage Europe-style attacks in U.S.

**By Christine Crowell, CNN**

**(CNN)** - ISIS has the capability to stage a Paris-style attack in the U.S. using local cells to strike in multiple locations and inflict dozens of casualties, according to the Obama administration's top U.S. intelligence official.

"That's something we worry about a lot in the United States," Director of National Intelligence James Clapper told CNN. "They could conjure up a raid like they did in Paris or Brussels," where March attacks on a train and at an airport left 32 dead and 300 people injured, Clapper said. The November 2015 Paris attacks killed at least 130.



*Law enforcement officers look over the evidence near the remains of the SUV involved in the December 2015 San Bernardino terrorist attack.*

Clapper said any attempted attack in the U.S. would echo the Europe assaults and, as in those cities, ISIS would "either infiltrate people or incite people who are already here." In a reference to the December 2015 shootings in San Bernardino, Calif., he added, "we've already seen some cases of that."

## Terror spread 'cause for serious concern'

U.S. officials' concerns are not unfounded. There was a 650 percent increase in fatal terror attacks on people living in the world's biggest economies over

the last few years, according to a report released by the Institute for Economics and Peace (IEP).

In 2015, there were 731 deaths related to terrorism in the 34 countries that make up the Organization for Economic Cooperation and Development, which includes the US, UK, Germany, France, and Turkey. The number represents the 650 percent increase on the previous year, with 21 of the 34 countries suffering at least one attack.

"The continued intensification of terrorism is a cause for serious concern and underscores the fluid nature of modern terrorist activity," IEP chief Steve Killelea said in a statement.

## Mass surveillance stops terror plots

Officials suggest one way to combat terrorism is through increased government surveillance of online and phone communications.

Former National Security Agency (NSA) Director Keith Alexander told CNN that phone and Internet surveillance programs thwarted approximately 50 terrorist plots. Mike Rogers, the former chairman of the House Intelligence Committee, affirmed that mass surveillance can prevent terrorist attacks in the U.S.

U.S. voters tend to agree, with 65 percent saying they believe the NSA's bulk data collection programs helped prevent terrorist attacks in the U.S., according to a CNN poll.

Voters can easily take action to combat terrorism by talking to state and federal legislators about passing laws that will allow for increased government surveillance in order to expose terrorist cells.

After the Paris terror attacks, Central Intelligence Agency Director John Brennan said terrorist operations can be uncovered and thwarted through the use of increased government surveillance.

"With the safety of U.S. citizens at stake, the administration is in 'relentless pursuit' of terrorist," Brennan said.

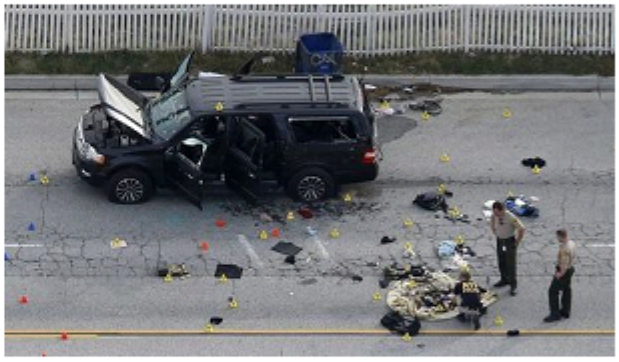
CNN

# Top U.S. intel official: ISIS can stage Europe-style attacks in U.S.

**By Christine Crowell, CNN**

ISIS has the capability to stage a Paris-style attack in the U.S. using local cells to strike in multiple locations and inflict dozens of casualties, according to the Obama administration's top U.S. intelligence official.

"That's something we worry about a lot in the United States," Director of National Intelligence James Clapper told CNN. "They could conjure up a raid like they did in Paris or Brussels," where March attacks on a train and at an airport left 32 dead and 300 people injured, Clapper said. The November 2015 Paris attacks killed at least 130.



*Law enforcement officers look over the evidence near the remains of the SUV involved in the December 2015 San Bernardino terrorist attack.*

Clapper said any attempted attack in the U.S. would echo the Europe assaults and, as in those cities, ISIS would "either infiltrate people or incite people who are already here." In a reference to the December 2015 shootings in San Bernardino, Calif., he added, "we've already seen some cases of that."

## Terror spread 'cause for serious concern'

U.S. officials' concerns are not unfounded. There was a 650 percent increase in fatal terror attacks on people living in the world's biggest economies over the last few years, according to a report released by the Institute for Economics and Peace (IEP).

In 2015, there were 731 deaths related to terrorism in the 34 countries that make up the Organization for Economic Cooperation and Development, which includes the US, UK, Germany, France, and Turkey. The number represents the 650 percent increase on the previous year, with 21 of the 34 countries suffering at least one attack.

"The continued intensification of terrorism is a cause for serious concern and underscores the fluid nature of modern terrorist activity," IEP chief Steve Killelea said in a statement.

## Mass surveillance cannot stop terror plots

Officials suggest one way to combat terrorism is through increased government surveillance of online and phone communications.

However, a report by New American's International Security Program suggests the government's claims about the role of bulk surveillance in keeping the U.S. safe from terrorism are overblown and even misleading.

The group's in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group demonstrated that traditional investigative methods, such as the use of informants, tips from local communities and targeted intelligence operations provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal.

The group said there is no proof that bulk surveillance programs stopped any terrorist attacks.

Civil rights activists tell CNN that it would be difficult for the American people, individually, to attempt to combat terrorism using increased mass surveillance. To do that, Congress would need to pass laws that provide government intelligence agencies with heighted surveillance power.

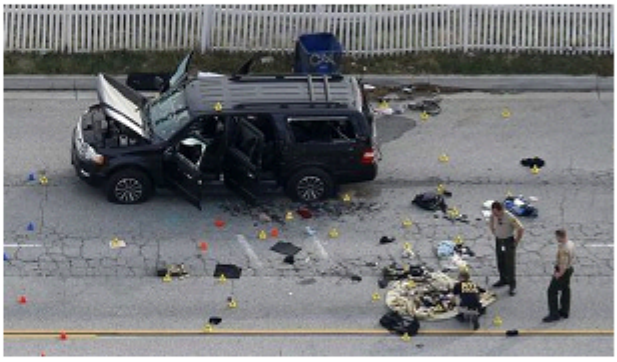
CNN

# Top U.S. intel official: ISIS can stage Europe-style attacks in U.S.

**By Christine Crowell, CNN**

ISIS has the capability to stage a Paris-style attack in the U.S. using local cells to strike in multiple locations and inflict dozens of casualties, according to the Obama administration's top U.S. intelligence official.

"That's something we worry about a lot in the United States," Director of National Intelligence James Clapper told CNN. "They could conjure up a raid like they did in Paris or Brussels," where March attacks on a train and at an airport left 32 dead and 300 people injured, Clapper said. The November 2015 Paris attacks killed at least 130.



*Law enforcement officers look over the evidence near the remains of the SUV involved in the December 2015 San Bernardino terrorist attack.*

Clapper said any attempted attack in the U.S. would echo the Europe assaults and, as in those cities, ISIS would "either infiltrate people or incite people who are already here." In a reference to the December 2015 shootings in San Bernardino, Calif., he added, "we've already seen some cases of that."

## Terror spread 'cause for serious concern'

U.S. officials' concerns are not unfounded. There was a 650 percent increase in fatal terror attacks on people living in the world's biggest economies over the last few years, according to a report released by the Institute for Economics and Peace (IEP).

In 2015, there were 731 deaths related to terrorism in the 34 countries that make up the Organization for Economic Cooperation and Development, which includes the US, UK, Germany, France, and Turkey. The number represents the 650 percent increase on the previous year, with 21 of the 34 countries suffering at least one attack.

"The continued intensification of terrorism is a cause for serious concern and underscores the fluid nature of modern terrorist activity," IEP chief Steve Killelea said in a statement.

## Reporting suspicious activity stops terror plots

According to the Department of Homeland Security (DHS), one of the best ways to combat terrorism is by reporting suspicious activity to law enforcement.

"Informed, alert communities play a critical role in keeping our nation safe," DHS spokesperson Marsha Catron said.

The agency promotes a campaign called "If You See Something, Say Something," which calls on individuals to keep any eye out for suspicious activity and report it to authorities.

DHS stressed that each person's daily routine is unique and there are many opportunities to notice when something seems off.

It is easy for a person to contact the police if he or she notices a strange package in a public area or an individual who is acting suspicious.

"If you see something you know shouldn't be there, or someone's behavior that doesn't seem quite right, say something," Catron said. "Because only you know what's supposed to be in your everyday."

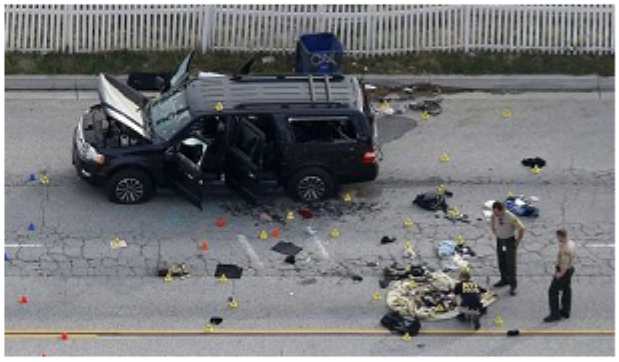
Top intelligence officials agree that individuals can uncover and thwart terrorist activities by monitoring their surroundings and reporting suspicious activity.

# Top U.S. intel official: ISIS can stage Europe-style attacks in U.S.

**By Christine Crowell, CNN**

ISIS has the capability to stage a Paris-style attack in the U.S. using local cells to strike in multiple locations and inflict dozens of casualties, according to the Obama administration's top U.S. intelligence official.

"That's something we worry about a lot in the United States," Director of National Intelligence James Clapper told CNN. "They could conjure up a raid like they did in Paris or Brussels," where March attacks on a train and at an airport left 32 dead and 300 people injured, Clapper said. The November 2015 Paris attacks killed at least 130.



*Law enforcement officers look over the evidence near the remains of the SUV involved in the December 2015 San Bernardino terrorist attack.*

Clapper said any attempted attack in the U.S. would echo the Europe assaults and, as in those cities, ISIS would "either infiltrate people or incite people who are already here." In a reference to the December 2015 shootings in San Bernardino, Calif., he added, "we've already seen some cases of that."

## Terror spread 'cause for serious concern'

U.S. officials' concerns are not unfounded. There was a 650 percent increase in fatal terror attacks on people living in the world's biggest economies over the last few years, according to a report released by the Institute for Economics and Peace (IEP).

In 2015, there were 731 deaths related to terrorism in the 34 countries that make up the Organization for Economic Cooperation and Development, which includes the US, UK, Germany, France, and Turkey. The number represents the 650 percent increase on the previous year, with 21 of the 34 countries suffering at least one attack.

"The continued intensification of terrorism is a cause for serious concern and underscores the fluid nature of modern terrorist activity," IEP chief Steve Killelea said in a statement.

## Reporting suspicious activity cannot stop terror plots

According to the Department of Homeland Security (DHS), one way to combat terrorism is by reporting suspicious activity to law enforcement.

However, critics suggest there is little evidence that individual reporting can prevent terrorism.

Tips to the Federal Bureau of Investigation (FBI) regarding Omar Mateen did not prevent him from walking into a packed nightclub in Orlando, Fla., massacring 49 people and wounding dozens more in the worst mass shooting in U.S. history.

The bureau gets tens of thousands of tips each year from people reporting suspicious activity, said an FBI spokesperson. Most are discarded after rudimentary investigation.

Often, people are unable to provide a name or other identifying information about suspicious individuals, which makes it difficult for authorities to investigate further.

It can also be difficult to determine whether an individual is truly acting suspicious or if a package was planted or simply forgotten.

These issues can make individual reporting of suspicious activity difficult.

CNN

# US says 75% of ISIS fighters killed

**By Christine Crowell, CNN**

**(CNN)** - At least 75% of ISIS fighters have been killed during the campaign of US-led airstrikes, according to US officials.

The US anti-ISIS envoy said the campaign has winnowed ISIS' ranks to between 12,000 and 15,000 "battle ready" fighters, a top US official said.

The figures mean the US and its coalition partners have taken out vastly more ISIS fighters in Iraq and Syria than currently remain on the battlefield, two years since the bombing campaign began. Last week a US official said the coalition had killed 50,000 militants since 2014.

CIA Director John Brennan participates in a session at the 3rd annual Intelligence and National Security Summit in Washington, DC

Speaking at the White House, Brett McGurk, the US special envoy to the anti-ISIS coalition, said the terror group is no longer able to replenish its ranks, predicting the number of fighters would continue to dwindle.

The Obama administration has been in "relentless pursuit" of ISIS, John Brennan, director of the Central Intelligence Agency, told CNN.

Brennan touted the administration's efforts against terrorist groups, which include a coalition of more than 60 countries to attack ISIS's financial and oil infrastructure, stemming the flow of foreign fighters joining them in Syria and Iraq, and training Iraqi and Kurdish soldiers to help in the battle.

Brennan said he is confident that ISIS will be wiped out.

"Doomed," he said. "It's just a matter of time."

## Reduction in global deaths due to terrorism

The coalition's efforts appear to be working.

A new study published by the Institute of Economics and Peace, shows that globally there was a decrease in deaths from terrorism.

According to the 2016 Global Terrorism Index, across the world as a whole, the number of deaths from terrorism fell 10% to 29,376, compared to the previous year.

## Mass surveillance stops terror plots

Officials suggest one way to combat terrorism is through increased government surveillance of online and phone communications.

Former National Security Agency (NSA) Director Keith Alexander told CNN that phone and Internet surveillance programs thwarted approximately 50 terrorist plots. Mike Rogers, the former chairman of the House Intelligence Committee, affirmed that mass surveillance can prevent terrorist attacks in the U.S.

U.S. voters tend to agree, with 65 percent saying they believe the NSA's bulk data collection programs helped prevent terrorist attacks in the U.S., according to a CNN poll.

Voters can easily take action to combat terrorism by talking to state and federal legislators about passing laws that will allow for increased government surveillance in order to expose terrorist cells.

After the Paris terror attacks, Central Intelligence Agency Director John Brennan said terrorist operations can be uncovered and thwarted through the use of increased government surveillance.

"With the safety of U.S. citizens at stake, the administration is in 'relentless pursuit' of terrorist," Brennan said.

# US says 75% of ISIS fighters killed

**By Christine Crowell, CNN**

**(CNN)** - At least 75% of ISIS fighters have been killed during the campaign of US-led airstrikes, according to US officials.

The US anti-ISIS envoy said the campaign has winnowed ISIS' ranks to between 12,000 and 15,000 "battle ready" fighters, a top US official said.

The figures mean the US and its coalition partners have taken out vastly more ISIS fighters in Iraq and Syria than currently remain on the battlefield, two years since the bombing campaign began. Last week a US official said the coalition had killed 50,000 militants since 2014.

CIA Director John Brennan participates in a session at the 3rd annual Intelligence and National Security Summit in Washington, DC

Speaking at the White House, Brett McGurk, the US special envoy to the anti-ISIS coalition, said the terror group is no longer able to replenish its ranks, predicting the number of fighters would continue to dwindle.

The Obama administration has been in "relentless pursuit" of ISIS, John Brennan, director of the Central Intelligence Agency, told CNN.

Brennan touted the administration's efforts against terrorist groups, which include a coalition of more than 60 countries to attack ISIS's financial and oil infrastructure and training Iraqi and Kurdish soldiers to help in the battle.

Brennan said he is confident that ISIS will be wiped out.

"Doomed," he said. "It's just a matter of time."

## Reduction in global deaths due to terrorism

The coalition's efforts appear to be working.

A new study published by the Institute of Economics and Peace, shows that globally there was a decrease in deaths from terrorism.

According to the 2016 Global Terrorism Index, across the world as a whole, the number of deaths from terrorism fell 10% to 29,376, compared to the previous year.

## Mass surveillance cannot stop terror plots

Officials suggest one way to combat terrorism is through increased government surveillance of online and phone communications.

However, a report by New American's International Security Program suggests the government's claims about the role of bulk surveillance in keeping the U.S. safe from terrorism are overblown and even misleading.

The group's in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group demonstrated that traditional investigative methods, such as the use of informants, tips from local communities and targeted intelligence operations provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal.

The group said there is no proof that bulk surveillance programs stopped any terrorist attacks.

Civil rights activists tell CNN that it would be difficult for the American people, individually, to attempt to combat terrorism using increased mass surveillance. To do that, Congress would need to pass laws that provide government intelligence agencies with heighted surveillance power.

CNN

# US says 75% of ISIS fighters killed

**By Christine Crowell, CNN**

**(CNN)** - At least 75% of ISIS fighters have been killed during the campaign of US-led airstrikes, according to US officials.

The US anti-ISIS envoy said the campaign has winnowed ISIS' ranks to between 12,000 and 15,000 "battle ready" fighters, a top US official said.

The figures mean the US and its coalition partners have taken out vastly more ISIS fighters in Iraq and Syria than currently remain on the battlefield, two years since the bombing campaign began. Last week a US official said the coalition had killed 50,000 militants since 2014.

CIA Director John Brennan participates in a session at the 3rd annual Intelligence and National Security Summit in Washington, DC

Speaking at the White House, Brett McGurk, the US special envoy to the anti-ISIS coalition, said the terror group is no longer able to replenish its ranks, predicting the number of fighters would continue to dwindle.

The Obama administration has been in "relentless pursuit" of ISIS, John Brennan, director of the Central Intelligence Agency, told CNN.

Brennan touted the administration's efforts against terrorist groups, which include a coalition of more than 60 countries to attack ISIS's financial and oil infrastructure, stemming the flow of foreign fighters joining them in Syria and Iraq, and training Iraqi and Kurdish soldiers to help in the battle.

Brennan said he is confident that ISIS will be wiped out.

"Doomed," he said. "It's just a matter of time."

## Reduction in global deaths due to terrorism

The coalition's efforts appear to be working.

A new study published by the Institute of Economics and Peace, shows that globally there was a decrease in deaths from terrorism.

According to the 2016 Global Terrorism Index, across the world as a whole, the number of deaths from terrorism fell 10% to 29,376, compared to the previous year.

## Reporting suspicious activity stops terror plots

According to the Department of Homeland Security (DHS), one of the best ways to combat terrorism is by reporting suspicious activity to law enforcement.

"Informed, alert communities play a critical role in keeping our nation safe," DHS spokesperson Marsha Catron said.

The agency promotes a campaign called "If You See Something, Say Something," which calls on individuals to keep any eye out for suspicious activity and report it to authorities.

DHS stressed that each person's daily routine is unique and there are many opportunities to notice when something seems off.

It is easy for a person to contact the police if he or she notices a strange package in a public area or an individual who is acting suspicious.

"If you see something you know shouldn't be there, or someone's behavior that doesn't seem quite right, say something," Catron said. "Because only you know what's supposed to be in your everyday."

Top intelligence officials agree that individuals can uncover and thwart terrorist activities by monitoring their surroundings and reporting suspicious activity.

CNN

# US says 75% of ISIS fighters killed

**By Christine Crowell, CNN**

**(CNN)** - At least 75% of ISIS fighters have been killed during the campaign of US-led airstrikes, according to US officials.

The US anti-ISIS envoy said the campaign has winnowed ISIS' ranks to between 12,000 and 15,000 "battle ready" fighters, a top US official said.

The figures mean the US and its coalition partners have taken out vastly more ISIS fighters in Iraq and Syria than currently remain on the battlefield, two years since the bombing campaign began. Last week a US official said the coalition had killed 50,000 militants since 2014.

CIA Director John Brennan participates in a session at the 3rd annual Intelligence and National Security Summit in Washington, DC

Speaking at the White House, Brett McGurk, the US special envoy to the anti-ISIS coalition, said the terror group is no longer able to replenish its ranks, predicting the number of fighters would continue to dwindle.

The Obama administration has been in "relentless pursuit" of ISIS, John Brennan, director of the Central Intelligence Agency, told CNN.

Brennan touted the administration's efforts against terrorist groups, which include a coalition of more than 60 countries to attack ISIS's financial and oil infrastructure, stemming the flow of foreign fighters joining them in Syria and Iraq, and training Iraqi and Kurdish soldiers to help in the battle.

Brennan said he is confident that ISIS will be wiped out.

"Doomed," he said. "It's just a matter of time."

## Reduction in global deaths due to terrorism

The coalition's efforts appear to be working.

A new study published by the Institute of Economics and Peace, shows that globally there was a decrease in deaths from terrorism.

According to the 2016 Global Terrorism Index, across the world as a whole, the number of deaths from terrorism fell 10% to 29,376, compared to the previous year.

## Reporting suspicious activity cannot stop terror plots

According to the Department of Homeland Security (DHS), one way to combat terrorism is by reporting suspicious activity to law enforcement.

However, critics suggest there is little evidence that individual reporting can prevent terrorism.

Tips to the Federal Bureau of Investigation (FBI) regarding Omar Mateen did not prevent him from walking into a packed nightclub in Orlando, Fla., massacring 49 people and wounding dozens more in the worst mass shooting in U.S. history.

The bureau gets tens of thousands of tips each year from people reporting suspicious activity, said an FBI spokesperson. Most are discarded after rudimentary investigation.

Often, people are unable to provide a name or other identifying information about suspicious individuals, which makes it difficult for authorities to investigate further.

It can also be difficult to determine whether an individual is truly acting suspicious or if a package was planted or simply forgotten.

These issues can make individual reporting of suspicious activity difficult.

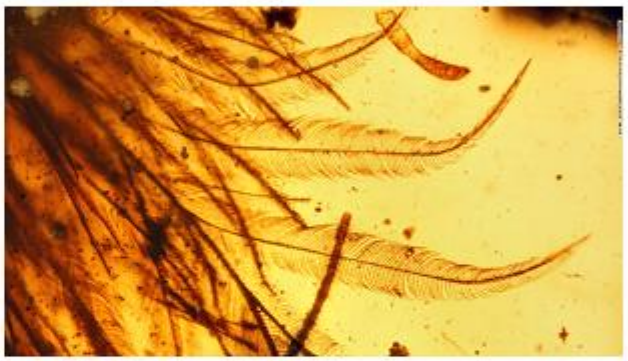
CNN

# 'Once in a lifetime find': Dinosaur tail discovered trapped in amber

**By Christine Crowell, CNN**

**(CNN)** - The tail of a 99-million-year-old dinosaur has been found entombed in amber, an unprecedented discovery that has blown away scientists.

Xing Lida, a Chinese paleontologist found the specimen, the size of a dried apricot, at an amber market in northern Myanmar near the Chinese border.



*The amber adds to fossil evidence that many dinosaurs sported feathers rather than scales.*

The remarkable piece was destined to end up as a curiosity or piece of jewelry, with Burmese traders believing a plant fragment was trapped inside.

"I realized that the content was a vertebrate, probably theropod, rather than any plant," Xing told CNN.

"I was not sure that (the trader) really understood how important this specimen was, but he did not raise the price."

## 'Once in a lifetime find'

The findings, which shed fresh light on how dinosaurs looked, are published in the newest issue of Current Biology.

Ryan McKellar, a paleontologist at the Royal Saskatchwan Museum in Canada, says he was blown away when Xing first showed him the piece of amber.

"It's a once in a lifetime find. The finest details are visible and in three dimensions."

Fragments of dinosaur-era bird wings have been found preserved in amber before but this is the first time part of a mummified dinosaur skeleton has been discovered, McKellar said.

The tail section belongs to a young coelurosaurian -- from the same group of dinosaurs as the predatory velociraptors and the tyrannosaurus. The sparrow-sized creature could have danced in the palm of your hand.

The amber, which weighs 6.5 grams, contains bone fragments and feathers, adding to mounting fossil evidence that many dinosaurs sported primitive plumage rather than scales.

## No scaly monster

McKellar said the creature would have had a whip-like tail like a mouse but covered with contour feathers similar to those that give shape and color to birds.

"The more we see these feathered dinosaurs and how widespread the feathers are, things like a scaly velociraptor seem less and less likely and they've become a lot more bird like in the overall view," he said. "They're not quite the Godzilla-style scaly monsters we once thought."

The amber preserved pigmentation from the feathers allowing the scientists to assess with some certainty how it looked. Seen under a microscope, the feathers suggest the creature was chestnut brown and white.

"It underlines the importance of amber as an anchor for future study. We're picking up features we couldn't see in compressed sedimentary fossils," McKellar said.

In the "Jurassic Park" movie franchise, scientists extract dinosaur DNA from blood found inside insects preserved in amber. McKellar said soft tissue and decayed blood from the tail were found in the amber but no genetic material was preserved.

"Unfortunately, the Jurassic Park answer is still a 'no' -- this is firmly in the realm of science fiction," he said.

**References for Stimuli**

Carroll, R. (2015, April 22). "NSA surveillance needed to prevent ISIS attack, claims former intelligence chair" *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2015/apr/22/mass-surveillance-needed-isis-attack-mike-rogers.

Center for Strategic and International Studies. (2015). *Global Security Forum 2015: Opening Session*. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/151116_GSF_OpeningSession.pdf.

Fox, K., Gilbert, D. (2016, Nov. 16). "Terror attacks in developing world surge 650% in one year." *CNN*. Retrieved from http://www.cnn.com/2016/11/16/world/global-terrorism-report/index.html

Gaouette, N. (2016, May 4). "Top U.S. intel official: ISIS can stage Europe-style attacks in U.S." *CNN*. Retrieved from http://www.cnn.com/2016/05/04/middleeast/obama-clapper-isis-attack-u-s-soil/

Homeland Security. (n.d.). If you See Something, Say Something: About the Campaign. Retrieved from https://www.dhs.gov/see-something-say-something/about-campaign

Nelson, S. (2013, June 18). "NSA Director: Surveillance Stopped 50 Terror Plots." *U.S. News*. Retrieved from http://www.usnews.com/news/newsgram/articles/2013/06/18/nsa-director-surveillance-stopped-50-terror-plots.

Reilly, K. (2016, May 4) "Top U.S. Intelligence Official: ISIS Has 'Capacity' for Paris-Style Attack In U.S." *Time.* Retrieved from http://time.com/4318165/isis-national-security-threat-obama/

Sherfinski, D. (2015, June 4). "NSA surveillance prevented terrorist attacks, most voters say: poll" *The Washington Times*. Retrieved from http://www.washingtontimes.com/news/2015/jun/4/nsa-surveillance-prevented-terrorist-attacks-poll/

Wilber, D.Q. (2016, July 14). "The FBI investigated the Orlando mass shooter for 10 months – and found nothing. Here's why." *Los Angeles Time*. Retrieve from http://www.latimes.com/nation/la-na-fbi-investigation-mateen-20160712-snap-story.html

## References

ACLU v. Clapper – Challenge to NSA Mass Call-Tracking Program. (2015, October 29). Retrieved from https://www.aclu.org/cases/aclu-v-clapper-challenge-nsa-mass-call-tracking-program.

*Am. Civ. Liberties Union v. Clapper*, 785 F.3d 787, 802 (2d Cir. 2015).

Acquisti, A. (2004, May). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce* (pp. 21-29). ACM.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, (1), 26-33.

Altman, I. (1976). Privacy:" A Conceptual Analysis." *Environment and behavior*, *8*(1), 7.

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006, May). Privacy and contextual integrity: Framework and applications. In *Security and Privacy, 2006 IEEE Symposium on* (pp. 15-pp). IEEE.

Basil, M., Basil, D., Deshpande, S., & Lavack, A. M. (2013). Applying the Extended Parallel Process Model to workplace safety messages. *Health communication*, *28*(1), 29-39.

Bambauer, D. E. (2013). Privacy versus security. *J. Crim. L. & Criminology*, *103*, 667.

Benner, K. & Lichtblau, E. (2016, March 15). "Apple and Justice Dept. Trade Barbs in iPhone Privacy Case." *New York Times*. Retrieved from http://www.nytimes.com/2016/03/16/technology/apple-court-filing-iphone-case.html?_r=0.

Blass, M. (2014). New Data Marketplace: Protecting Personal Data, Electronic Communications, and Individual Privacy in the Age of Mass Surveillance through a Return to a Property-Based Approach to the Fourth Amendment, The. *Hastings Const. LQ*, *42*, 577.

Brooks, R (20, November 2015). "The Threat is Already Inside," *Foreign Policy*. Retrieved from https://foreignpolicy.com/2015/11/20/the-threat-is-already-inside-uncomfortable-truths-terrorism-isis/.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157-165.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk a new source of inexpensive, yet high-quality, data?. *Perspectives on psychological science*, *6*(1), 3-5.

Burkell, J., Fortier, A., Wong, L. L. Y. C., & Simpson, J. L. (2014). Facebook: Public space, or private space?. *Information, Communication & Society*, *17*(8), 974-985.

*Cantrell v. Forest City Pub. Co.*, 419 U.S. 245, 248 (1974).

Carroll, R. (2015, April 22). "NSA surveillance needed to prevent ISIS attack, claims former intelligence chair" *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2015/apr/22/mass-surveillance-needed-isis-attack-mike-rogers.

Christensen, G. (2006). Government Information Collection: Federal Data Collection, Secure Flight, the Intelligence Reform and Terrorism Prevention Act, and the Reauthorization of the USA PATRIOT Act. ISJLP, 2, 485-981.

Chong, D., & Druckman, J. N. (2011). Identifying frames in political news. *Sourcebook for Political Communication Research: Methods, Measures, and Analytical Techniques*, 238-67.

de Vreese, C., Peter, J., & Semetko, H.A. (2001). Framing politics at the launch of the Euro: A cross-national comparative study of frames in the news. *Political communication*, *18*(2), 107-122.

Duggan, M., & Smith, A. (2013). 'Social Media Update 2013,' *Pew Research Center Report*, [Online] Available at: http://pewinternet.org/Reports/2013/Social-Media-Update.aspx.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), 1143-1168.

Eoyang, M. (2016). Beyond Privacy & Security: The Role of the Telecommunications Industry in Electronic Surveillance. *National Security, Technology, and Law*. A *Hoover Institution Essay*. Retrieved from http://www.hoover.org/research/beyond-privacy-security-role-telecommunications-industry-electronic-surveillance-0.

Facebook says government requests for user data rises 24 pct. (2014, Nov. 4). Retrieved from http://www.reuters.com/article/2014/11/04/facebook-data-idUSL4N0SU6TB2014 1104

Farr, C. and Oreskovic, A. (2014, October 3), "Facebook plots first steps into healthcare," *Reuters*. Retrieved from http://www.reuters.com/article/2014/10/03/us-facebook-health-idUSKCN0HS09720141003].

Finkel, J. (2016, February 25). "Solid support for Apple in iPhone encryption fight: poll" *Reuters*. Retrieved from http://in.reuters.com/article/us-apple-encryption-poll-idINKCN0VX159.

FISA, 50 U.S.C. § 1881 (2008).

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. Journal of applied social psychology, 30(2), 407-429.

Florek, A. (2013). Problems with PRISM: How a Modern Definition of Privacy Necessarily Protects Privacy Interests in Digital Communications, *J. Marshall J. Info. Tech. & Privacy L.*, *30*, 571.

Frizell, S. (2015, December 15). "Hillary Clinton Calls for More Surveillance for Fight Terror" *Time.* Retrieved from http://time.com/4150694/hillary-clinton-calls-for-more-surveillance-to-fight-terror/.

Garner, B. A. (Ed.). (2006). *Black's law dictionary Pocket Edition* (3rd ed.). St. Paul, MN: Thomson Reuters.

Gass, R. H., & Seiter, J. S. (2015). *Persuasion: Social influence and compliance gaining* (3rd Ed.) Boston: Pearson Education Inc.

Goodall, C. E., & Reed, P. (2013). Threat and efficacy uncertainty in news coverage about bed bugs as unique predictors of information seeking and avoidance: An extension of the EPPM. *Health communication*, *28*(1), 63-71.

Gore, T. D., & Bracken, C. C. (2005). Testing the theoretical design of a health risk message: reexamining the major tenets of the extended parallel process model. *Health Education & Behavior*, *32*(1), 27-41.

Gormley, K. (1992). One hundred years of privacy. *Wis. L. Rev.*, 1335.

Gosling, S. D., Vazire, S., Srivastava, S., & John, O. P. (2004). Should we trust web-based studies? A comparative analysis of six preconceptions about internet questionnaires. *American Psychologist*, 59(2), 93.

Henry, L. (2015). Information Privacy and Data Security. *Cardozo Law Review de Novo*.

Hong, H. (2011). An extension of the extended parallel process model (EPPM) in television health news: the influence of health consciousness on individual message processing and acceptance. *Health communication*, 26(4), 343-353.

*Katz v. United States*, 389 U.S. 347 (1967).

Kim, S., Jeong, S. H., & Hwang, Y. (2012). Predictors of pro-environmental behaviors of American and Korean students: The application of the theory of reasoned action and protection motivation theory. *Science Communication*, 1075547012441692.

Knobloch-Westerwick, S., Johnson, B. K., & Westerwick, A. (2013). To Your Health: Self-Regulation of Health Behavior Through Selective Exposure to Online Health Messages. *Journal of Communication*, *63*(5), 807-829.

Knobloch-Westerwick, S., & Meng, J. (2009). Looking the other way selective exposure to attitude-consistent and counterattitudinal political information. *Communication Research*, *36*(3), 426-448.

*Kyllo v. United States*, 533 U.S. 27 (2001).

Litman, J. (2000). Information privacy/information property. *Stanford Law Review*, 1283-1313.

Maloney, E. K., Lapinski, M. K., & Witte, K. (2011). Fear appeals and persuasion: A review and update of the extended parallel process model.*Social and Personality Psychology Compass*, *5*(4), 206-219.

McCarthy, T (2015, December 6). "Surveillance must increase after terror attacks, say 2016 candidates," *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2015/dec/06/paris-attacks-san-bernardino-shooting-surveillance-hillary-clinton-donald-trump-election.

McMahan, S., Witte, K., & Meyer, J. A. (1998). The perception of risk messages regarding electromagnetic fields: extending the extended parallel process model to an unknown risk. *Health communication*, *10*(3), 247-259.

Metzger, M. J., Hartsell, E. H., & Flanagin, A. J. (2015). Cognitive Dissonance or Credibility? A Comparison of Two Theoretical Explanations for Selective Exposure to Partisan News. *Communication Research*, 0093650215613136.

Miners, Z. (2014). "As the tentacles of Facebook's data spread, privacy questions resurface," *CIO*, October 3 [available at http://www.cio.com.au/article/556611/tentacles-facebook- data-spread-privacy-questions-resurface/].

Muthusamy, N., Levine, T. R., & Weber, R. (2009). Scaring the already scared: Some problems with HIV/AIDS fear appeals in Namibia. *Journal of Communication*, *59*(2), 317-344.

Napolitano, A. P. (2013). Legal History of National Security Law and Individual Rights in the United States: The Unconstitutional Expansion of Executive Power, The. NYUJL & Liberty, 8, 396.

Nelson, S. (2013, June 18). "NSA Director: Surveillance Stopped 50 Terror Plots." *U.S. News*. Retrieved from http://www.usnews.com/news/newsgram/articles/2013/06/18/nsa-director-surveillance-stopped-50-terror-plots.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, *79*, 119.

*Olmstead v. United States*, 222 U.S. 438 (1928).

*Pavesich v. New England Life Ins. Co.* 69 L.R.A. 101, 122 Ga. 190, 50 S.E. 68, 106 Am.St.Rep. 104 (Ga. 1905)

Palmer, S. (2013, August 16). PRISM: There Simply is No Privacy... None. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/shelly-palmer/prism-there-simply-is-no_b_3451721.html

Petronio, S. (2002). Boundaries of privacy. State University of New York Press, Albany, NY.

Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication*, *13*(1), 6-14.

Popova, L. (2012). The Extended Parallel Process Model Illuminating the Gaps in Research. *Health Education & Behavior*, *39*(4), 455-473.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods*, 40, 879-891.

Prosser, W. L. (1960). Privacy. *Cal. L. Rev.*, *48*, 383.

Rainie, L. & Duggan, M. (2016). Privacy and Information Sharing. *Pew Research Center*. Retrieved from: http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

Riles, J. M., Sangalang, A., Hurley, R. J., & Tewksbury, D. (2015). Framing Cancer for Online News: Implications for Popular Perceptions of Cancer. *Journal of Communication*, 65(6), 1018-1040.

Roberto, A. J., & Goodall, C. E. (2009). Using the extended parallel process model to explain physicians' decisions to test their patients for kidney disease. *Journal of health communication*, *14*(4), 400-412.

Roskos-Ewoldsen, D. R., Yu, J. H., & Rhodes, N. (2004). Fear appeal messages affect accessibility of attitudes toward the threat and adaptive behaviors. *Communication Monographs*, 71(1), 49-69.

Rogers, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R.E. Petty (Eds.). *Social Psychophysiology* (pp. 153-176). New York: Guilford.

Rushe, D. (2014), "Facebook sorry – almost – for secret psychological experiment on users," *The Guardian*, October 2. Retrieved from http://www.theguardian.com/technology/2014/oct/02/facebook-sorry-secret-psychological-experiment-users].

Schneier, B. (2014, March 13). "Metadata = Surveillance," Schneier on Security. Retrieved from https://www.schneier.com/blog/archives/2014/03/metadata_survei.html.

Scheier, B. (2015, November 24). "NSA Collected Americans' E-mails Even After it Stopped Collecting Americans' E-mails," Schneier on Security. Retrieved from https://www.schneier.com/blog/archives/2015/11/nsa_collected_a.html.

Schneier, B. (2016, January 7). "Straight Talk about Terrorism," Schneier on Security. Retrieved from https://www.schneier.com/blog/archives/2016/01/straight_talk_a.html.

Schneier, B., Seidel, K., Vijayakumar, S. (2016). A Worldwide Survey of Encryption Products. Retrieved from https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf.

Schwartz, P. M. (2012). Information privacy in the cloud. *U. Pa. L. Rev.*, *161*, 1623.

Selyukh, A. & Domonoske, C. (2016, February 17). "Apple, the FBI and iPhone Encryption:A Look at What's at Stake." *NPR*. Retrieved from http://www.npr.org/sections/thetwo-

way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake.

Semetko, H.A., & Valkenburg, P.M. (2000). Framing European politics: A content analysis of press and television news. *Journal of Communication*, 50(2), 93-109.

Smith, A. (2014). 6 new facts about Facebook. *Pew Research Center*. Retrieved from http://www.pewresearch.org/fact-tank/2014/02/03/6-new-facts-about-facebook/.

Smith, S. W., Rosenman, K. D., Kotowski, M. R., Glazer, E., McFeters, C., Keesecker, N. M., & Law, A. (2008). Using the EPPM to create and evaluate the effectiveness of brochures to increase the use of hearing protection in farmers and landscape workers. *Journal of Applied Communication Research*, *36*(2), 200-218.

*Smith v. Maryland*, 442 U.S. 735 (1979)

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, 1087-1155.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania law review*, 477-564.

Solove, D. J. (2008). Understanding privacy. Harvard University Press, Cambridge, Mass.

Solove, D. J. (2008). The new vulnerability: data security and personal information. In *Securing Privacy in the Internet Age*. (Radin & Chander, Eds). Stanford University Press.

Sydell, L. (2012), "Yet Another Shift in Facebook Policies Raises Privacy Concerns," *NPR*, November 29. Retrieved from http://www.npr.org/blogs/alltechconsidered/2012/11/29/166177278/yet-another-shift-in-facebook-policies-raises-privacy-concerns.

Tankard, J. W. (2001). The empirical approach to the study of media framing. In S.D. Reese, O.H. Gandy & A. E. Grant (Eds.), *Framing public life: Perspectives on media and our understanding of the social world*, 95-106. Mahwah, NJ: Lawrence Erlbaum.

Trager, R., Russomanno, J., Ross, S. D., & Reynolds, A. (2013). *The law of journalism and mass communication*. CQ Press.

Trepte, S., & Reinecke, L. (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Springer Science & Business Media.

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, *51*(5), 546-562.

*United States v. Chadwick*, 433 U.S. 1 (1977)

Vara, V. (2014), "Facebook's Targeted Ads Expand to the Web," *The New Yorker*, September 30 [available at http://www.newyorker.com/business/currency/facebook-targeted-ads-raise-new-privacy-questions].

Westerwick, A., Kleinman, S. B., & Knobloch-Westerwick, S. (2013). Turn a blind eye if you care: Impacts of attitude consistency, importance, and credibility on seeking of political information and implications for attitudes.*Journal of Communication*, *63*(3), 432-453.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of social issues*, *59*(2), 431-453.

Wikimedia v. NSA – Challenge to Upstream Surveillance under the FISA Amendment's Act. (2015, October 23). Retrieved from https://www.aclu.org/cases/wikimedia-v-nsa-challenge-upstream-surveillance-under-fisa-amendments-act?redirect=national-security/wikimedia-v-nsa.

*Wikimedia Foundation, et al., Plaintiffs--Appellants, v. National Security Agency, et al., Defendants--Appellees*, 2016 WL 703452 (C.A.4), 1-2.

Witte, K. (1993). Message and conceptual confounds in fear appeals: The role of threat, fear, and efficacy. *Southern Journal of Communication*, *58*(2), 147-155.

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs*, *61*(2), 113-134.

Witte, K. (1997). Preventing teen pregnancy through persuasive communications: realities, myths, and the hard-fact truths. *Journal of community health*, *22*(2), 137-154.

Witte, K. (2000). *EPPM: Examples of items*. Retrieved from https://msu.edu/~wittek/scale.htm.

Witte, K., Cameron, K.A., McKeon, J.K., Berkowitz, J.M. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of health communication*, *1*(4), 317-342.

Witte, K., Berkowitz, J. M., Cameron, K. A., & McKeon, J. K. (1998). Preventing the spread of genital warts: Using fear appeals to promote self-protective behaviors. *Health Education & Behavior*, *25*(5), 571-585.

Yanovitzky, I. (2002). Effects of News Coverage on Policy Attention and Actions A Closer Look Into the Media-Policy Connection. *Communication research*, *29*(4), 422-451.

Zetter, K (2013, June 27). "Under Obama , NSA Collected Bulk Email, Internet Data of Americans," *Wired*. Retrieved from https://www.wired.com/2013/06/nsa-collected-bulk-u-s-email/.

# Vita

Angela Rulffes is a Ph.D. candidate at the S.I. Newhouse School of Public Communications. Her research is focused on the evolution of free speech and privacy rights in the digital age. Before coming to Syracuse University, she worked as an editor of a legal real estate publication. Angela is a licensed New York State attorney. During and after law school, Angela worked as an attorney and law clerk for the ACLU of Ohio, focusing on civil liberties issues including free speech rights. She has a JD from Cleveland-Marshall College of Law, an MS in Broadcast Journalism from Syracuse University and a BA in English from SUNY Plattsburgh.