1-1-2011

The relationship between cell phone use and identity theft

Lewis O. Saunders
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Lewis Saunders

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Raj Singh, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Walter McCollum, Committee Member,
Public Policy and Administration Faculty

Dr. Wendy Andberg, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2014

Abstract

The Relationship Between Cell Phone Use and Identity Theft

by

Lewis O. Saunders

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

March 2014

Abstract

The growth of mobile phone use has paralleled increased reports of identity theft. Identity theft can result in financial loss and threats to a victim's personal safety. Although trends in identity theft are well-known, less is known about individual cell phone users' attitudes toward identity theft and the extent to which they connect it to cell phone use. The purpose of this qualitative study was to determine how cell phone use is affected by attitudes toward privacy and identity theft. The study was based on social impact theory, according to which people's attitudes and behavior are affected by the strength and immediacy of others' attitudes and behavior. The research questions concerned the extent to which participants connected cell phone use with decreasing privacy and increasing cybercrime, how the use of biometrics affected cell phone users' attitudes and behavior, and what steps can be taken to reduce the misuse of private information associated with cell phone use. Data collection consisted of personal interviews with representatives from 3 groups: a private biometrics company, individual cell phone users who earn more than $55,000 a year, and individual cell phone users who earn less than $55,000 a year. Interviews were transcribed and coded for themes and patterns. Findings showed that interviewees were more likely to see identity theft as a problem among the public at large than in the industries in which they worked. Participants recommended a variety of measures to improve cell phone security and to reduce the likelihood of identity theft: passwords, security codes, voice or fingerprint recognition, and encryption. The implications for positive social change include informing government officials and individual users about the use and abuse of cell phones in order to decrease violations of privacy and identity theft while still promoting national security.

The Relationship Between Cell Phone Use and Identity Theft

by

Lewis O. Saunders

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

March 2014

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

Dedication

I dedicate this analytical effort to my mother, Frances J. Roy Saunders, who has been a guiding light in my pursuit for higher education. Additionally, special gratitude is given to my wife, Rachel, who has provided comments and corrections when, to my belief, everything seems to be perfect. Thanks to our children, Valera, Sarita, and Cassandra, who provided support and encouragements throughout the entire process of receiving my Ph.D.

Acknowledgements

Special thanks and deep appreciation to my mentor and chair, Dr. Raj Singh. Without his special guidance I would have not been able to reach the goal I have planned and hoped for since I was a boy. I am also grateful for the help and advice of Dr. Walter McCollum, who assisted me in applying to Walden University and recommended books to read. Thank you Dr. Iran Birdsall for serving on one of the most important parts of any dissertation or study by assuring that the methodology can produce sound and useful results.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

Introduction

Few individual rights are important to people in the United States as the right of privacy. Privacy is defined by Weitzner (2007) as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 96). Privacy is threatened by the pace of technological development. One example of that development is cell phone use. Cell phone subscriptions increased from 97 million in 2000 to over 331 million at the beginning of 2012 (Cellular Telecommunications and Internet Association [CTIA], 2012). Cell phones, noted Akin (2009), have the potential to threaten privacy because monitoring devices can be placed in the software of a cell phone without the owner's knowledge, allowing someone else to track the owner's conversations and locations. Lost or stolen cell phones also leave users vulnerable to a loss of privacy. The misuse of private data can lead to crimes such as robbery and kidnapping (Kim & Hong, 2008).

An example of the difficulty of protecting cell phone users' privacy is using biometrics for voice authentication. Pocovinicu (2009) noted that biometrics can be used by banks to establish that callers are who they say they are. A caller is asked to recite a pass phrase, and that vocal rendition is compared to a sample collected earlier. As Riley, Buckner, Johnson, and Benyon (2009) pointed out, however, the use of biometrics adds to the amount and kinds of information about private citizens that are gathered and stored, and storing personal information creates the possibility for its misuse.

Identity theft, defined by Milne (2003) as "the appropriation of someone else's personal or financial identity to commit fraud or theft" (pp. 389-392), has emerged as the

most frequent U.S. consumer complaint, far ahead of debt collection (see Figure 1). Identity theft can be accomplished in many ways (e.g., stealing mail, stealing credit cards, stealing Social Security numbers). Consumer complaints about identity theft peaked in 2008 and declined over the next 2 years (see Figure 2).

Consumer Sentinel Network
Complaint Categories[1]
January 1 – December 31, 2010

Rank	Category	No. of Complaints	Percentages[1]
1	Identity Theft	250,854	19%
2	Debt Collection	144,159	11%
3	Internet Services	65,565	5%
4	Prizes, Sweepstakes and Lotteries	64,085	5%
5	Shop-at-Home and Catalog Sales	60,205	4%
6	Impostor Scams	60,158	4%
7	Internet Auction	56,107	4%
8	Foreign Money Offers and Counterfeit Check Scams	43,866	3%
9	Telephone and Mobile Services	37,388	3%
10	Credit Cards	33,258	2%
11	Advance-Fee Loans and Credit Protection/Repair	31,726	2%
12	Banks and Lenders	29,967	2%
13	Credit Bureaus, Information Furnishers and Report Users	28,724	2%
14	Mortgage Foreclosure Relief and Debt Management	28,584	2%
15	Television and Electronic Media	28,245	2%
16	Business Opportunities, Employment Agencies and Work-at-Home Plans	24,123	2%
17	Health Care	21,710	2%
18	Computer Equipment and Software	20,833	2%
19	Travel, Vacations and Timeshare Plans	18,836	1%
20	Auto Related Complaints	15,787	1%
21	Magazines and Books	10,994	1%
22	Home Repair, Improvement and Products	10,435	1%
23	Office Supplies and Services	9,367	1%
24	Investment Related Complaints	6,430	<1%
25	Grants	4,382	<1%
26	Real Estate	4,337	<1%
27	Charitable Solicitations	3,314	<1%
28	Clothing, Textiles and Jewelry	2,850	<1%
29	Multi-Level Marketing, Pyramids and Chain Letters	2,187	<1%
30	Video Games	1,353	<1%

[1]Percentages are based on the total number of CSN complaints (1,339,265) received by the FTC between January 1 and December 31, 2010. Thirteen percent (176,565) of the total CSN complaints received by the FTC were coded Other (Note in Comments). For CSN category descriptions, details and three year figures, see Appendices B1 through B3.

Figure 1. Consumer complaints in 2010. From the Federal Trade Commission Consumer Sentinel Network (FTCCST; 2011). Used with permission.

Calendar Year	Consumer Sentinel Network Complaint Count			Total Complaints
	Fraud	Identity Theft	Other	
2001	137,306	86,250	101,963	325,519
2002	242,783	161,977	146,862	551,622
2003	331,366	215,240	167,051	713,657
2004	410,298	246,909	203,176	860,383
2005	437,585	255,687	216,042	909,314
2006	423,672	246,214	236,243	906,129
2007	503,797	259,314	303,039	1,066,150
2008	609,595	314,521	316,970	1,241,086
2009	680,704	278,356	418,785	1,377,845
2010	725,087	250,854	363,324	1,339,265

[1] Complaint counts from CY-2001 to CY-2005 represent historic figures as per the Consumer Sentinel Network's five-year data retention policy. These complaint figures exclude National Do Not Call Registry complaints.

Figure 2. Consumer complaints 2001-2010. From the FTCCST (2011). Used with permission.

Problem Statement

Identity theft has become the most frequent consumer complaint in the United States (FTCCST, 2011). The potential for identity theft has increased with the growth of cell phone use. Adams and Dimitrinu (2008) noted that cell phones contribute to a social phenomenon whereby people leave "rich information footprints that are easily accessible to others, reducing the currency of private information for authentication purposes" (p. 23). By manipulating the touch screen on a cell phone, for example, financial data can be transferred to banks and other financial institutions.

Although people are concerned about identity theft, there is some evidence that definitions of privacy are changing. Tian, Shi, and Yang (2009) studied attitudes toward mobile phones among 3,021 Chinese cell phone users. Tian et al. found that cell phone use reflects three attitudes: security, character extension, and dependence. Tian et al. defined security as "the mobile phone's [perceived] ability to reduce uncertainty and bring safety" (p. 513) and claimed that a reason for using mobile devices is a concern for

personal safety. Tian et al. attributed this attitude to what they called *character extension*, a phenomenon whereby a cell phone functions not only as a communication tool but also as an extension of one's physical self. Tian et al. cited personalized background images and special ring tones as examples of character extension. Demographic characteristics of their sample are summarized in Table 1.

Table 1

Demographic Information of the Sample

Age (years)	Number	Percentage	Gender	Number	Percentage
10-15	13	0.4	Male	2,133	70.6
16-24	785	26.0	Female	888	29.4
25-34	1,232	40.8	Occupation		
35-44	577	19.1	Employee	951	31.5
45-54	277	9.2	Manager	351	9.7
55-64	94	3.1	Official	85	2.8
65-70	22	0.7	Industry worker	359	11.9
Missing	21	0.7	Teacher/Doctor/Police officer	118	3.9
Monthly Income (RMB)			Student		
< 2,000	1,067	35.3	Technician	189	6.3
2,001-4,000	909	30.1	Private merchant	285	9.4
4,001-6,000	296	9.8	Farming/fishery	78	2.6
6,001-8,000	83	2.7	Retired/unemployed	69	2.3
8,001-10,000	50	1.7	Voluntarily unemployed	221	7.3
More than 10,000	102	3.4	Other	128	4.2
Missing	514	17.0	Missing	44	1.5

Note. From Tian, Shi, and Yang (2009). Used with permission.

Although the extent of cell phone use has been documented (CTIA, 2010), users' attitudes toward those devices is less well known. In particular, there is a gap in knowledge regarding the extent to which cell phone users are concerned about loss of

privacy connected with cell phone use. Much is known about trends in identity theft (FTCCST, 2011), but little is known about whether cell phone owners connect their cell phone use to an increased risk of identity theft. A lack of consumer awareness regarding the vulnerability of cell phone users to identity theft and related crimes could make it easier for criminals to operate. Several researchers have called for additional research in these areas (Brenner, 2010; King & Jessen, 2010; Morris, 2010), and that gap in the literature is the problem addressed in this study.

Nature of the Study

This qualitative study is appropriate for investigations based on people's experiences (Glaser, 2004; Polkinghorne, 2005). Specifically, this study was phenomenological, which is more descriptive than analytical. Phenomenological researchers study everyday experiences, behavior, and relationships (Moustakas, 1994). A quantitative study was also considered, which would have accommodated a larger sample. Quantitative researchers typically use surveys or other instruments with data that can be statistically analyzed. Qualitative research, however, permits greater depth, which is appropriate for a study based on people's experiences and attitudes.

Examples of qualitative research designs are biographical studies, ethnographies, and case studies. Biographical research might take the form of an oral history (Roberts, 2002). A biographical study is confined to a single participant. Although such a design permits an in-depth exploration of one person's experience and opinions, its narrow focus would not have been appropriate for this study, which was an attempt to gain a broader perspective on a phenomenon.

Ethnography is an attempt to portray a way of life from the participants' point of view. Creswell (2007) described an ethnography as "a description and interpretation of a cultural or social group or system" based on "the group's observable and learned patterns of behavior, customs, and ways of life" (p. 58). Typically, ethnographic research is based on observation and interviews. Although this study involved interviews, the purpose was not to understand the way of life of the respondents, but to explore their experience and perspectives regarding a particular phenomenon.

A case study is "an exploration of a case (or cases) over time through detailed, in-depth data collection involving multiple sources of information rich in context" (Creswell, 2007, p. 61). The current study overlaps with a case study design in that multiple sources of information were sought. However, whereas the purpose of a case study is to explore the internal dynamics of a particular group, environment, or situation, the focus of the current study was not on the workings of a group but on their attitudes regarding a particular phenomenon.

In a phenomenological study, a researcher attempts to describe "the meaning of lived experiences for several individuals about a concept or phenomenon" (Creswell, 2007, p. 51). This design was the most appropriate form of qualitative research for the current study. The lived experience of cell phone users is precisely what I explored. This phenomenological study was based on personal interviews with representatives from three groups: a biometrics company, individual cell phone users earning more than $55,000 annually, and individual cell phone users earning less than $55,000 annually. The purpose was to gauge industry and consumer attitudes regarding the relationship between cell phone use and loss of privacy and identity theft. Participants lived or

worked in the Baltimore, Maryland–Washington, D.C. corridor. The study was based on Moustakas's (1994) seven-step process for conducting phenomenological research, which is described further in Chapter 3. Interview results were transcribed and coded for themes based on key words and phrases using NVivo software.

Research Questions

This study was based on three research questions:

1. To what extent do biometrics industry representatives and individual cell phone users connect cell phone use with decreasing privacy and identity theft?
2. How is cell phone users' behavior affected by their attitudes toward privacy and identity theft?
3. What steps can be taken to reduce the incidence of identity theft associated with cell phone use?

Purpose of the Study

The purpose of this study was to explore how attitudes toward privacy and identity theft affected the behavior of cell phone users. Whether the U.S. Constitution guarantees a right to privacy has been debated by legal scholars, but the Constitution has been consistently interpreted to prevent unreasonable searches of private property and government intrusion into what are generally considered private relationships, such as that between parents and children. With the growing popularity of social media such as Facebook, Twitter, and Foursquare, there is some evidence that attitudes toward privacy are changing (Butler, McCann, & Thomas, 2011; Cowan, 2010; Grimmelmann, 2010;

Veer, 2010). Collecting personal data on consumers is an advantage to businesses, which can use that information for targeted marketing (Wirtz & Lwin, 2009).

Cell phones provide a record of users' locations. When cell phones are equipped with global positioning systems (GPS), that location can be pinpointed with accuracy. The availability of such information to others has caused some concerns for its potential to lead to crimes such as robbery and kidnapping (Brenner, 2010; Gershowirt, 2011; Stilton, 2009). This study will lead to a better understanding of the potential for misuse of cell phones and how that potential affects the attitudes of biometrics industry representatives, and private citizen cell phone users.

Theoretical Framework

This study was based on social impact theory, first developed by Latané (1981). According to Latané, a social impact is any situation in which people affect each other's attitudes and behavior. More specifically, Latané suggested that social impact is affected by the strength and immediacy of other's attitudes and behavior, and by the number of people involved. Strength is, in turn, affected by judgments people make about the source of impact: age, social class, status, and so forth.

The advent of personal computers—in the form of desktops, laptops, tablets, smart phones, and other personal digital assistants (PDAs)—has transformed the workplace as well as people's personal lives. The penetration of such devices into U.S. society is evidence of their utility in peoples' work and social lives. At the same time, the growing presence of personal computers and the resulting ease with which information can be shared, captured, and stored has increased the potential for personal information to be misused (Brenner, 2010; Gershowirt, 2011; Stilton, 2009).

The term *cybercrime* has been used to refer broadly to any instance in which an individual or group uses computers to gain unauthorized access to other computers for personal gain (Akopyan & Yelyako, 2009). A specific form of cybercrime is *phishing*, whereby potential victims receive a message from what looks like an official source, asking for personal information (Akopyan & Yelyako, 2009, p. 338). Cybercrime, by definition, involves the misuse of computers and information technology. Some crimes are not unique to computer use but have been made easier because of the potential access to information that the computer provides. For example, identity theft is a crime that can be committed by stealing mail, purses, or wallets. But whereas a criminal operating that way would have to commit numerous individual thefts to create multiple fraudulent identities, a cybercriminal could accomplish the same thing with a single theft of a large database. Similarly, crimes such as robbery and kidnapping have existed throughout human history. With the advent of cell phones, though, especially those equipped with GPS, tracking a person's location could make it easier for a criminal to commit various crimes against persons (Brenner, 2010; Gershowirt, 2011; Stilton, 2009). The examples of cybercrime cited this far suggest a certain degree of intentionality. But the size and transportability of PDAs make them easy to lose, and finding a PDA—with its store of information such as names, addresses, phone numbers, e-mail messages, and photos—creates an opening for a crime of opportunity (Kim & Hong, 2008). Other crimes, such as robbery, could proliferate based on the happenstance knowledge that someone is not home at a given time.

There are over 331 million cell phone subscriber connections in the United States (CITA, 2012). Further, cell phones are becoming much more than phones; indeed, the so-

called smart phone is, in effect, a pocket or purse computer. What is less clear is how people's attitudes toward privacy and personal information have been affected by cell phone use, and how those attitudes affect vulnerability to various forms of crime.

Definitions of Terms

Application (app): Software that can be used on mobile devices for connecting to the World Wide Web through a specified brand of smart phone or mobile device (Charland & Leroux, 2011).

Biometrics: The uses of physical or behavioral traits, such as fingerprints, face, voice, and hand geometry, to establish an individual's identity (Jain, Flynn, & Ross, 2008).

Cloud computing: A networked online system for remote storage of electronic information and software (O'Brien & Marakas, 2011).

Cybercrime: Any form of crime conducted using computers and the Internet (Joseph, 2006).

Data literacy: Facility in handling quantitative information in a variety of formats, including electronic (Hunt, 2004).

Identity theft: An impersonation of someone without that person's permission (LoPucki, 2003).

Information technology: A system of delivering information and services to users via computer (PC Magazine, 2012).

Participatory sensing: Surveillance that takes place with the knowledge and permission of the person being monitored (Stilton, 2009).

Phishing: A form of cybercrime whereby potential victims receive a message from what looks like an official source, asking for personal information (Akopyan & Yelyako, 2009).

Smartphone: A cell phone with built-in applications and Internet access. With a smart phone, a user can send and receive e-mail and browse the Web (PC Magazine, 2012).

Assumptions, Limitations, and Scope

I assumed that participants would provide accurate and honest responses to interview questions. Because it was based on interview data, this study was limited by participants' ability to recall details of their personal experience. It is possible that some participants, knowing the purpose of the study, slanted their responses to fulfill what they imagined to be my goals. This study was limited to a convenience sample of representatives from two groups: biometrics company employees and private citizens who are cell phone users. All participants lived or worked in the Washington, DC, area.

Significance of the Study

The use and abuse of information technology is affected by the prevailing political climate. For example, after the attacks of September 11, 2001, on the World Trade Center, the United States experienced heightened vigilance regarding national security. That concern gave rise to increased efforts by the federal government to monitor the behavior of private citizens; because electronic communication enabled by computers and mobile phones is traceable and the contents storable, the potential for surveillance of private communication among U.S. citizens and between U.S. citizens and those of other countries was enhanced.

The ability of the federal government to monitor electronic communication was broadened by the Patriot Act, first passed in 2001, reauthorized in 2006, and extended in 2011). Title II of the act expanded the government's ability to engage in wiretapping, and Title III empowered the Federal Bureau of Investigation (FBI) to search voicemail messages of anyone under suspicion (U.S. Patriot Act [U.S. H.R. 3162, Public Law 107-56]). The American Civil Liberties Union (ACLU; 2012) has been critical of the act, charging that it has been used to create "a surveillance superstructure" (para 2). The ACLU argued that there is little evidence that the Patriot Act has improved national security and evidence that the powers it granted have been misused.

The cultural climate also affects how people view personal information. The ease of sharing biographical data, opinions, photographs, and geographical location through such social media vehicles as Facebook, Twitter, and Foursquare has created a climate in which notions of privacy are changing. To the extent that people want others to know who they are, where they are, and what they think at any given moment, and to the extent that such information can be shared through a device they carry with them at all times, the consensus definition of privacy operative is likely different from what it has been (Brenner, 2010; Gershowirt, 2011; Stilton, 2009). This definition is likely different because not enough is known about how information technology has affected people's attitudes toward privacy. Although it is easy to determine how many people own cell phones and how often they access social media sites, it is more difficult to determine how those facts affect attitudes toward privacy. Yet, assessing people's attitudes is important if curtailments of electronic monitoring and information gathering are to be tightened or relaxed. In this study, I addressed a gap in what is known about how attitudes toward

privacy and cybercrime affect cell phone use. The study can effect social change by informing efforts of governmental agencies and private business to adapt policies to changing individual and social needs and behavior.

Summary

In this chapter, a qualitative study was described on how cell phone use is affected by attitudes toward privacy and cybercrime. The study was based on social impact theory, which suggests that individual attitudes and behavior are affected by the strength and immediacy of others' attitudes and behavior. A convenience sample of biometrics industry employees and individual cell phone users was interviewed. Results were coded for themes using NVivo software. The study can effect social change by revealing how notions of privacy are affected by cell phone use and by informing efforts to match government oversight with individual and business needs and desires.

In Chapter 2, the relevant literature on cell phones, social media, privacy, cybercrime, and government oversight will be reviewed. In Chapter 3, the study's methods, including research design, population and sample, data collection and analysis procedures, and ethical protections, will be described. In Chapter 4, the results are summarized, and Chapter 5 consists of conclusions and recommendations.

Chapter 2: Literature Review

Introduction

This chapter comprises a review of the relevant literature for a qualitative study of how cell phone use is affected by attitudes toward privacy and identity theft. In the review, I cover informational technology, privacy, security, biometrics, and surveillance, as well as the study's theoretical underpinnings. The review began with a search of the following databases: ProQuest, EBSCOhost, and the Walden University Research Library. Search terms included the following: *identity theft, cell phones, mobile phones, wireless technology,* and *privacy.*

Theoretical Framework

This study was based on social impact theory, which was first formulated by Latané (1981) and has been widely used in social science research (Argo, Dahl, & Machanda, 2005; Bourgeois & Bowen, 2001; Harton, Green, & Jackson, 1998; Nettle, 1999). Latané defined social impact as

> any of the great variety of changes in physiological states and subjective feelings, motives and emotions, cognitions and beliefs, values and behavior, that occur in an individual, human or animal, as a result of the real, implied, or imagined presence or actions of other individuals. (p. 343)

Social impact, according to Latané, is affected by the strength and immediacy of the forces to which an individual is subjected.

Nowak, Szamrej, and Latané (1990) noted that the relationship between individuals and groups is reciprocal. The function of social groups is influenced by the individual members of the group, and individuals in turn are affected by the dynamics of

the groups to which they belong. The key fact about social impact, Nowak et al. argued, is that "individuals in a given social context behave differently than they would outside that context" (p. 362).

Social impact theory is used to predict that an individual's behavior will be influenced by the "the real, implied, or imagined presence or actions of other individuals" (Latané, 1981, p. 343). In the context of the current study, the operative words in Latané's definition are *implied* and *imagined*. Although a person might use a cell phone in the presence of others, that act is something one does individually, and the object of that use — whether to engage others in electronically mediated communication, or to access information, or to play an electronic game—is usually pursued without the influence of others one can see. For a cell phone user, the presence or actions of others is implied or imagined. They constitute an imagined presence rather than a real one. Their influence, however, is no less significant for that fact, according to the tenets of social impact theory.

Someone engaged in a phone conversation can take steps to minimize the possibility that the conversation will be overheard: stepping outside, lowering one's voice, and so forth. In such a situation, it is the presence of others that influences an individual's behavior. However, it is possible that this hypothetical cell phone user's conversation is being monitored electronically, a fact of which he or she would be oblivious. The issue of privacy is further complicated when a smart phone is used to send e-mail, visit a website, or otherwise access electronic content. Any use of the Internet leaves an electronic trace, and one's perception or lack of perception about the implications of that trace can affect one's online behavior.

Orwell (1949) described the members of a fictional society called Oceania who were subjected to government surveillance by means of telescreens. The effect of that surveillance, according to the novel's narrator, was to make Oceanians internalize the effects of being watched and heard, whether they are actually being observed or not.

> There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. . . . You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized. (Orwell, 1949, pp. 6-7)

Bowers (1988) warned about the long-term, internalized effects of technology in reinforcing a cultural mindset that normalizes surveillance, monitoring, and data collection. Accepting such a state of affairs, Bowers cautioned, could become automatic and unconscious, seen as "essential to the development of the socially responsible citizen" (p. 122) and thus viewed as "a normal, even necessary, aspect of adult life" (p. 19). To the extent that Orwell's and Bowers's fears have been realized, cell phone users may have accepted whatever security risks their phone use poses as a necessary fact of life and may be vulnerable to exploitation by unscrupulous parties.

Information Technology

The explosion in information technology is evident in cell phone use, which in the United States increased from 97 million subscriptions in 2000 to over 331 million at the beginning of 2012 (CTIA, 2012). According to a 2011 Pew Research Center report, 81% of U.S. adults now own a cell phone (as cited in Smith, 2011). The cell phone has become much more than a telephone. In the Pew Research Center report, researchers

asked respondents to describe how they used a cell phone in the 30 days preceding the interview (as cited in Smith). Smith summarized some of their comments:

- Half of all adult cell phone owners (51%) had used their phone at least once to get information they needed right away. One quarter (27%) said they experienced a situation in the previous month when they had trouble doing something because they did not have their phone at hand.
- About 42% of cell phone owners used their phone for entertainment when they were bored.
- A fifth (20%) of cell phone owners experienced frustration because their phone was taking too long to download something.
- Nearly 13% of cell owners pretended to be using their phone in order to avoid interacting with the people around them.
- Three fourths of all cell phone owners (73%) used their phone for text messaging or picture taking. (p. 1)

Smith (2011) noted that alternative uses of cell phones have proliferated with the increasing sophistication of what are usually called *smart phones.* Table 2 shows how smart phone users compared to other cell phone users in the Pew survey.

Table 2

Smart Phone Users Versus Other Cell Phone Users

	Smart phone owners *n* = 688	Other cell phone owners *n* = 1.226
Send/receive texts	92%	59%
Take picture	92%	59%
Access Internet	84%	15%
Send photo/video	80%	36%
Send/receive e-mail	76%	10%
Download app	69%	4%
Play game	64%	14%
Play music	64%	12%
Record video	59%	15%
Access social networking	59%	8%
Watch video	54%	5%
Post photo/video	45%	5%
Do online banking	37%	5%
Access Twitter	15%	<1%
Participate in video call/chat	13%	1%

Note. From the Pew Research Center's *Internet and American Life Project*, April 26-May 22, 2011, Spring Tracking Survey. *N* = 2,277 adults ages 18 and older, including 755 cell phone interviews. Interviews were conducted in English and Spanish.

Privacy and Security

In an informational environment, there are concerns about both information privacy and intellectual property. According to Mayer-Schonberger (2010), both are based on individual rights. Mayer-Schonberger characterized information privacy rights as those that are subject to governance mechanisms. Because cell phones are increasingly being used to store a variety of personal information, concerns have arisen about the extent to which they constitute a security risk. However, public concern about the potential misuse of personal information predates the cell phone era, which began in the 1970s. According to Goldsborough (2010), "Despite its importance today, the word

'privacy' does not appear in the U.S. Constitution or Bill of Rights" (p. 72). According to Allen (2001), the modern concern with privacy began in the 1960s, when the Supreme Court introduced the idea of legal rights to privacy. Allen characterized current attitudes toward privacy as an obsession.

In the Fourth Amendment, the U.S. Constitution protects citizens from unreasonable search and seizure and states that search warrants can only be issued for probable cause. The Privacy Act (1974) addressed how the federal government collects, stores, and disseminates personal information. The act limits how and to what extent government agencies can disclose personally identifiable information. It covers individual records but does not address corporations. The Privacy Act states,

> No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains. (U.S. Department of Justice, 2003, p.36)

The Privacy Act also requires every government agency to institute a security system that prevents the unauthorized release of personal information.

Following the attacks on the World Trade Center in New York City on September 11, 2001, the United States made several changes to the original Privacy Act. In 2007, the administration of President George W. Bush instituted exemptions to the act for the Department of Homeland Security and the Automated Targeting System. Those agencies were given freedom to access personal data gathered for "immigrant and non-immigrant pre-entry, entry, status management and exit processes" relating to "national security, law enforcement, immigration and intelligence activities" (Statewatch, 2007, p. 29).

Since passage of the original Privacy Act, technological development has increased the ease with which personal information can be collected, stored, and distributed. Other legislation has been passed to control that process. The Electronic Communications Privacy Act (ECPA; 1986) was passed to clarify wiretapping and electronic eavesdropping provisions. ECPA has three components: the Wiretap Act, the Stored Communications Act, and the Pen-Register Act (Electronic Privacy Information Center [EPIC], 2012). The Wiretap Act includes oral communication, such as phone conversations. It "prohibits any person from intentionally intercepting or attempting to intercept a wire, oral or electronic communication by using any electronic, mechanical or other device" (as cited in EPIC, 2012, para 4). Exceptions include instances when consent of at least one party is given and when interception is authorized for law-enforcement purposes. Consent can be written into an employment contract, in which case an employer would not violate the Wiretap Act by listening to an employee's phone conversations.

Whereas the Wiretap Act has to do with intercepting electronic communication, the Stored Communications Act addresses such data after they have been stored. As such, it primarily concerns e-mail messages that are not in transit. This act makes it illegal to "obtain, alter, or prevent unauthorized access to a wire or electronic communication while it is in electronic storage" (as cited in EPIC, 2012, para 7). Like the Wiretap Act, it makes exceptions for user consent and access for law-enforcement purposes.

The Pen-Register Act covers devices that provide "non-content information about the origin and destination of particular communications" (as cited in EPIC, 2012, para 9). For phone calls, such information would include outgoing and incoming phone numbers.

The legislation applies to devices, including software, that capture such information. It grants access to local, state, and federal law enforcement agencies.

In addition to the provisions of ECPA, the government is free to collect certain kinds of information from communication providers. For example, a subpoena in the form of a national security letter "can be served on a company to compel it to disclose basic subscriber information" (EPIC, 2012, para 15). Such information might include subscriber name, address, and phone number(s); service start and stop times; and date and length of specific phone communications. This information is not supposed to include the actual content of any communications. In all cases, ECPA requires that if a government entity requests access to customer records, they must be "relevant and material to an ongoing criminal investigation" (EPIC, 2012, para 16) and when the provider "reasonably believes than an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information" (EPIC, 2012, para 17).

In addition to the matter of how electronic data should be used by law-enforcement entities in solving crime, questions have arisen about how the government should protect the electronic infrastructure on which national security depends. Bellovin, Bradner, Diffie, Sandau, and Rexford (2011) reported on government efforts to secure the Internet against threats from criminals bent on disabling the system. Bellovin et al. analyzed the effectiveness of a project called EINSTEIN, which was created in 2004 and has since gone through several iterations. The purpose of EINSTEIN was to collect and analyze computer information automatically to determine if looked suspicious, and, if so, make a report to the U.S. Computer Emergency Readiness Team. Bellovin et al. raised

concerns about threats to privacy posed by EINSTEIN, stating that the system is designed to intercept all communication from federal employees, including potentially private communication engaged in on a work computer. Bellovin et al. noted that although federal employees are similar to those at any company that supplies employees with equipment for electronic communication, EINSTEIN's monitoring would not be public. Bellovin et al. also raised questions about the reach of EINSTEIN, charging that although it was designed to protect federal agencies, there was interest in expanding it to other industries, including public utilities and communications. Bellovin et al. claimed that the data EINSTEIN collects could easily be misused, noting that whereas the federal system it was designed for serves 2 million employees; other systems would affect over 300 million people.

Cloud Computing

The advent of cloud computing, where electronic information is stored on a remote server rather than on a personal computer, has complicated the task of interpreting and applying ECPA. The National Institute of Standards and Technology (NIST) described cloud computing as a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (as cited in Mell & Grance, 2011, p. 2). The NIST definition consists of five essential characteristics, three service models, and four deployment models.

Essential Characteristics

- *On demand self-service*, enabling users to access computing capabilities automatically, without human interaction with service providers.
- *Broad network access*.
- *Resource pooling* of storage, processing, memory and network bandwidth.
- *Rapid elasticity* to accommodate changing demand.
- *Measured service,* whereby cloud systems automatically optimize resource use.

Service Models

- *Software as a service,* whereby users access a provider's applications running on cloud infrastructure.
- *Platform as a service,* whereby providers make available computing tools, libraries, programming languages, and so forth.
- *Infrastructure as a service,* where by users make use of operating systems and storage capacity.

Deployment Models

- *Private cloud,* provided for exclusive use by a single organization.
- *Community cloud,* provided for exclusive use by consumers from organizations with shared concerns.
- *Public cloud,* provided for open use by the general public.
- *Hybrid cloud,* a combination of all or some of the other models.

Cloud computing has grown rapidly in recent years. Cable & Wireless Worldwide reported that cloud computing grew over 60% from 2010 to 2011 and that 45% of

multinational corporations offered cloud-computing services in 2011, a 21% increase over the previous year (as cited in Lanois, 2011). Cloud computing makes it possible to store e-mails, photos, videos, and other electronic data on the Internet. This capability frees individual users from having to store large files on a personal computer and makes those files accessible from any networked electronic device, including smart phones.

Although cloud computing has led to greater convenience for Internet users, it has also raised privacy concerns. Lanois (2010) cited several recent controversies involving large social networking organizations, including Facebook, Google, and Twitter. A 2012 report by the Federal Trade Commission expressed concern about the ability of companies to monitor children's personal information based on applications on their cell phones (Lardner, 2012). Lardner reported that about 600 apps were available to smart phone users in 2008, whereas in 2010 almost 1 million apps existed and had been downloaded more than 29 billion times. He cited a report by Common Sense Media, a nonprofit group that studies children's use of technology. Their research found that more than half of U.S. children have access to smart phones, tablets, and other digital devices.

Another recent report, this one by Stanford University's Security Lab and the Center for Internet and Society, charged Google with circumventing privacy features built into Safari, the primary Web browser used on Apple's iPhone and iPad. Google did so, according to the report, by skirting the software's configurations that block third-party cookies (Perlberg, 2012). Cookies are small files created automatically when users access the Internet. They store information such as login names, but they also track a user's browsing history and thus can be used by online marketers to target users with particular interests (Lanois, 2010). As Lanois noted, "Cookies are relevant to cloud computing

since cookies are used for authentication purposes, such as identifying a server-based session, or storing and maintaining login and password information or similar data, administering the user's account, or identifying the browser used" (pp. 33-34).

According to a 2010 *Wall Street Journal* report, among the 50 most frequently accessed U.S. websites, accounting for 40% of the Web pages viewed by U.S. users, an average of 64 pieces of tracking technology were installed on users' electronic devices, often without their knowledge (Angwin, 2010). Much of the information collected in this way is then sold to third parties. Angwin noted that whereas previously users could limit such monitoring by removing the cookies that accumulate on their computer, more sophisticated tracking technology is making that more difficult. Angwin reported that monitoring software has become so powerful and widespread that some website designers are unaware that they have installed intrusive files on visitors' computers.

Growing alarm about the collection and sale of personal information acquired through people's Internet use has led to calls for greater government regulation. However, such calls have been met with claims by online businesses that more restrictive policies in this area could negatively affect an already fragile economy (Lanois, 2010). In the absence of federal legislation, Internet users have filed claims in district courts. In 2010, a California court approved a $9.5 million settlement in a class action suit against Facebook and its Beacon program. Beacon was an online advertisement system created to monitor the purchasing behavior of Facebook users (Lanois, 2010). Other recent examples include a 2010 class action suit filed against the online advertising company Quantcast. The plaintiffs claimed that Quantcast created cookies based on Adobe's Flash software to reconstruct cookies that users had previously deleted. Another 2010 lawsuit

charged Clearspring Technologies with hidden online surveillance by providing a web widget that tracks users' browsing behavior (Lanois, 2010).

A 2009 study about cookies and privacy found that 54 of the 100 most popular websites investigated used Flash cookies, but only four mentioned that fact in their privacy policies (Soltani, Canty, Mayo, Thomas, & Hoofnagle, 2009). Soltani et al. noted that Flash is not affected by browser controls for managing privacy. They concluded that a lack of disclosure on the part of Flash-using websites leaves consumers at the mercy of unwanted surveillance.

One complicating factor regarding security and cloud computing concerns jurisdiction. As Lanois (2010) noted, cloud computing renders geographical location irrelevant. Furthermore, Lanois observed, data security can vary considerably from one country to another, and most consumers who use cloud computing are unlikely to know where their personal information is stored. A 2009 report from the World Privacy Forum concluded that legal protections for cloud computing users have not kept up with technological advances (as cited in Gellman, 2009).

Sipior, Ward, and Mendoza (2011) noted that the original intent behind cookies was not to create a record of a user's browsing history but rather to enable a user to return to a particular site and resume interaction or complete a transaction. As the technology evolved, however, cookies and their spawn—Flash cookies and beacons—came to be used by Internet marketers and enabled them to target specific subsets of their audience with ads based on their preferences, as revealed in their browsing history. Flash cookies, unlike their predecessors, do not expire at the end of a session, and deleting them could compromise a user's ability to access Flash-dependent content on the Internet, where

75% of online videos are delivered by Flash technology and where most games and animation depend on Flash capability (Sipior et al., 2011).

Legislative Reform

Lanois (2010) argued that privacy law has not kept up with technological developments. He cited the recent creation of an initiative called Digital Due Process (DDP), constituting a coalition of lawyers, academics, technology companies, and civil rights organizations. The purpose of DDP is to update legislation that governs the accessibility of electronic data. One specific target of the coalition is ECPA, which DDP members believe should be reformed.

Although the Fourth Amendment would protect data stored on a computer or cell phone, whether it applies to data stored on a remote server is less clear. Uncertainty about the legal status of information stored in the cloud has led some observers to call for reforming ECPA (EPIC, 2012). For example, in 2011 Senator Patrick Leahy introduced a bill (S.1011) entitled the Electronic Communications Privacy Act Amendments Act of 2011. Among other provisions, it would require a warrant for seeking mobile phone location data. The bill was referred to the Committee on the Judiciary but has not yet been voted on (Library of Congress, 2012).

Kattan (2011) is another observer who has raised questions about the applicability of existing privacy legislation to protect users in an era of cloud computing. In addressing the applicability of the Fourth Amendment in an era of cloud computing, he noted that although the privacy of computer use in one's home has usually been upheld by the courts, data stored on a remote server are not always given the same legal protection. Specifically referencing the 1986 Stored Communications Act (SCA), which was part of

ECPA, Kattan stated that there is growing uncertainty about the act's adequacy for present conditions. After surveying the current state of affairs, Kattan proposed that Congress amend SCA.

Evolving attitudes and rapid technological development led King and Jessen (2010) to review the provisions of recent federal legislation, including the Electronic Communication Privacy Act and Computer Fraud and Abuse Act, as well as 2009 recommendations by the U.S. Federal Trade Commission (FTC). They concluded that existing electronic privacy policies are inadequate, and they formulated five recommendations to govern the use of personally identifiable information (PII) by companies:

1. Create a comprehensible and succinct privacy policy detailing their PII practices.
2. Post a conspicuous link to any privacy statement.
3. Disclose the external uses of PII (either collected actively or passively).
4. Disclose visitor consent options regarding PII collection and dissemination and privacy policy amendments.
5. Refrain from widely disseminating PII to the highest bidder on the open market. (p. 469)

Third-Party Use of Personal Data

King and Jessen (2010) noted that by tracking a person's electronic transactions, retailers can build a profile of a given individual and use it to tailor ads to that person's preferences. The researchers expressed concern about the potential for profiling to compromise individual privacy by interfering with "personal data protection" and

"personal autonomy and liberty" (p. 458). The cell phone, King and Jessen observed, generates more PII than other sources, including geographic location. Calling history, personal contacts, and the content of e-mail messages are subject to misappropriation. King and Jessen concluded that the ability of online companies to profile consumer behavior automatically enables them to circumvent government regulations on information collection and use. They called for more research in this area.

The issue of how companies use customer information for what has been called *relationship marketing* prompted a study by Wirtz and Lwin (2009) in which they distinguished between two approaches that businesses use: building trust, which they labeled proactive, and reducing concerns, which they characterized as defensive. Wirtz and Lwin proposed regulatory focus theory as a way of integrating these two approaches and examining their effectiveness. The purpose of relationship marketing is to build long-term relationships with customers and promote customer loyalty. This approach requires collecting personal information, which is easy for companies to do by tracking the electronic footprints left by users of various electronic devices. When people use credit cards, loyalty cards, ATMs, cell phones, and online services, they leave an electronic record of their behavior. A marketing department can hire a commercial service to collect and collate such information. Wirtz and Lwin cited one such service, Experian, which described its services as follows:

> We can help you to build a richer picture of your customers' behavior so you can predict and engineer how they behave in the future. Using internal and external data sources, our proven customer management tools allow you to tailor strategies to an individual. (as cited in Wirtz & Lwin, 2009, p. 192)

One danger in company collecting information about its clients is the possibility of security breaches. Wirtz and Lwin cited two recent examples of large-scale breaches: Bank of America Corporation, which lost tapes containing personal information for 1.2 million customers, and TJX Company, which had 45 million credit cards and debit card numbers stolen from its data storage system.

Although personal electronic information is potentially available through a variety of media, the telephone represents a unique source. As Wicker (2011) noted, tapping a phone invades the privacy of both the caller and the person who was called. Furthermore, Wicker observed, the fact that smart phones now hold a variety of data, including images and Web-browsing histories, makes them an attractive source of information for law enforcement personnel.

Stilton (2009) noted that the multiple functions of cell phones (microphone, camera, GPS, Internet access) make them potentially "the most widespread embedded surveillance tools in history" (p. 48). Stilton distinguished between *coercive* and *participatory* sensing. The former is typically referred to as surveillance and takes place without users' knowledge. Participatory sensing also involves collecting data, but that collecting is done with users' awareness and potential cooperation.

An example of participatory sensing is a project by UCLA's Center for Embedded Networked Sensing (CENS) called the personal environmental impact report (PEIR). The project was designed to enable Los Angeles, California, residents to monitor their exposure to air pollution and to estimate their carbon footprint. Based on participants' location, which is determined by a GPS-equipped phone, the PEIR system determines their probable activity (driving, riding public transit, biking, walking) at any given time

and assesses the air quality of their specific location based on regional data. Being able to determine someone's location at any given time enables CENS personnel to provide more accurate information about specific environmental threats.

Other CENS projects include Biketistic, where bicycling commuters carry microphone-, accelerometer-, and GPS-equipped cell phones on their daily commutes. The phone tracks a biker's route, roughness of the road, and noise volume. That information is automatically uploaded to a website, where participants can later observe their route and compare its conditions to other possible routes. The project's goal is to enable cyclists to plan their commutes to best fit their personal needs and desires (Stilton, 2009).

Although one enters into participatory sensing voluntarily, the experience is not without privacy risks. Stilton (2009) noted that privacy concerns include where and for how long personal data are stored, as well as what those data reveal about a person. Stilton also observed that location data could reveal such sensitive information as how often one consults a therapist, where one's child goes to school, or how often one is late to work. Such information could be misused by potential thieves, stalkers, or kidnappers. But beyond its potential to aid those intent on doing one harm, data that reveal one's movements, Stilton argued, could make people think twice about engaging in activities that are perfectly legal. Stilton asked, "Would you be as likely to attend a political protest, or visit a plastic surgeon, if you knew your location was visible to others?" (p. 50).

Stilton (2009) noted that legal protections of individual privacy concern personal data collection undertaken by government or other public entities. Protecting individual

privacy in an environment where a wealth of personal information is potentially available to observers outside of government, she argued, necessitates involving people in their own privacy decision making, which she called "participatory privacy regulation" (p. 51). To facilitate such a process, Stilton proposed three principles that should govern mobile data-gathering efforts:

- Giving participants as much control over their personal data as possible. This approach could involve creating a *personal data vault* for storing private data.
- Rendering personal data in ways that participants can easily understand. Such an effort could include graphical representations such as maps and charts.
- Making clear how long data will be stored and how long and under what conditions participants will have access to that information.

Stilton (2009) argued that although the challenge of responsible data management has been complicated by technological advances, trying to meet that challenge solely through technological means would be short-sighted and ultimately ineffective. "Participant engagement in privacy decision making," Stilton claimed, "needs to be fortified by supporting structures, as well" (p. 53). The goal, Stilton stated, is *data literacy*, a process that takes time and the involvement of many parties using a variety of communication tools: Listservs, blogs, discussion forums, community groups, and traditional media. She proposed a labeling system, like those used for food projects (e.g., those labeled organic or fair trade) that would inform consumers of what data-protection practices are followed by a given entity.

Another field that has taken advantage of participatory sensing is health care. Boulos, Wheeler, Tavares, and Jones (2011) noted that mobile phones have been used to collect data for health care research, to facilitate health-related community education, and to enable telemedicine and remote health care. Specific studies have explored the use of mobile phones by health care providers to help patients manage behavioral change, conduct sexual health education, and improve patients' adherence to medication regimes. Boulos et al. reported on the development of a smart phone health care app (eCAALYS) for use by elderly patients with multiple chronic diseases. The app enables patients to report information on their health status and receive alerts from a health care provider. The app can be integrated with sensor data from, say, a pacemaker.

True participatory privacy regulation depends on users' awareness of how their personal information is being used. As Grimmelmann (2010) noted, participation in social networking sites can give users the illusion that their behavior takes place in private space. Butler et al. (2011) studied the privacy concerns and awareness of Facebook users. Facebook is the world's largest social networking site, with over 500 million active users. Facebook's privacy policies have undergone numerous revisions since its inception, and with each change users are notified with a dialog box at the top of the screen, which has a link to more information. One question is how many users take the time to read the new policy and act on it.

According to Butler et al. (2011), Facebook has regularly modified its default privacy settings, adopting an opt-out approach whereby users must indicate if they want more privacy than the default settings provide. Veer (2010) charged that "Facebook assumes you want the whole world to see your personal info until you tell it differently.

Your information is at risk until you adjust your settings" (p. 209). Facebook's privacy page has had as many as 50 settings and 170 options, raising the question of whether most users understand it (Cowan, 2010).

The reason people use social networking sites like Facebook is because they want to share information with others. According to Butler et al. (2011), however, many Facebook users are probably unaware of the implications of sharing personal information in such a forum. As Grimmelmann (2010) noted, Facebook profiles typically include information that prospective employees cannot ask applicants for a job, including religion, gender, race, and marital status. "People are voluntarily uploading it all because they are social and because Facebook scratches social itches" (Grimmelmann, 2010, p. 811). "Overall," concluded Butler et al., "it seems users care more about making an identity for themselves on the social networking site, than managing who can view that identity" (p. 46).

To assess Facebook users' knowledge of and attitudes toward the site's privacy policies, Butler et al. (2011) administered a 25-item survey to 235 Facebook users, most of whom were 18-30 years of age. The sample was 63% female and 37% male. When asked if they had read Facebook's privacy policy, 14% checked "Yes, I am aware of the latest version," 17% said "Yes, but only when I first created my account," 27% said "I have only read parts of it," 29% responded "No, I have never read it, but I know where to find it if needed," and 12% said "No, I have never read it, and I don't even know where to find it if needed." Although the majority of users admitted either partial or total unfamiliarity with Facebook's current privacy policy, the majority agreed with the

statement, “I am confident that I understand and am aware of my personal privacy settings on Facebook.”.

In response to a question about whether they believed Facebook adequately protected their privacy, 70% of participants answered yes. Asked who could view personal content they posted, 82% of participants said it was only viewable by their “friends”—that is, other Facebook users the participant had approved. However, 58% reported having one or more friends they had never met. Based on the data they collected, Butler et al. (2011) concluded that Facebook users are not well-informed about the site’s privacy policies and are largely unaware of the potential consequences of their ignorance.

Brenner (2010) noted that a wide range of private and public activities are increasingly dependent on electronic systems and lamented the absence of concrete governmental action to address what he characterized as the nation’s increasing vulnerability to misuse of those systems. Brenner quoted extensively from government documents to illustrate his claim that little has been done in the last 20 years to improve cybersecurity. For example, in 1990, the Bush administration issued a national security directive that stated the following: “Telecommunications and information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well a other dimensions of the foreign intelligence threat” (as cited in Brenner, 2010, p. 33). Almost 20 years later, the Obama administration issued a report stating the following:

> The architecture of the Nation’s digital infrastructure, based largely on the Internet, is not secure or resilient. Without major advances in the security of these systems or significant change in how they are constructed or operated, it is

> doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations. (as cited in Brenner, 2010, p. 33)

Why, asked Brenner, has so little been done in 20 years?

Brenner (2010) expressed little confidence in the ability of the market to drive improvements in cybersecurity. Instead, he argued that government should assume a more active role by taking the following eight steps:

1. Use its purchasing power to require higher security standards from its vendors.
2. Amend the Privacy Act to require that Internet service providers (ISPs) inform customers when their data security has been compromised.
3. Define conditions that would permit ISPs to block or sequester data transmission.
4. Forbid federal agencies from doing business with any ISP that is a hospitable host for suspect Internet-based entities.
5. Require bond issuers to disclose whether their supervisory control and data acquisition networks are connected to the Internet or other publicly accessible network.
6. Increase support for research into techniques that would improve cybersecurity.
7. Remove antitrust threats facing U.S. companies that cooperate on researching, developing, or implementing security functions.

8. Engage like-minded foreign governments to create international agreements that would enhance cybersecurity.

Identity Theft

A specific misuse of PII is identity theft. According to the U.S. Department of Justice (2011), "Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain" (para 1). The Identity Theft Assumption and Deterrence Act of 1998 (ITADA) defined identity theft as follows:

> Knowingly transfer[ing] or us[ing], without lawful authority, any name or number that may be used, alone or in conjunction with any other information, to identity a specific individual with any other information, to identity a specific individual with the intent to commit or aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law (United States Public Law 105-318). (as cited in Morris, 2010, p. 186)

Morris noted that this definition includes such criminal activities as credit fraud and check fraud, which now are identified as identity theft based on the assumption that criminals use information about someone other than themselves. Despite these definitions, Morris claimed that the absence of a consensus agreement about what constitutes identity theft has created confusion and inconsistency regarding which law enforcement entities have authority to investigate suspected cases. Morris added that many victims are content to be reimbursed for their losses without enduring the complex process that filing a legal claim would involve.

Five years ago, Roberts and Schreft (2009) estimated the total cost of identity theft, including direct losses and money spent prosecuting the crimes, at $61 billion a year. This amount is likely to have increased from 2009 to 2013. Besides the quantifiable costs of identity theft, there is the inconvenience suffered by its victims, who may be subject to threatening letters and phone calls, demands for payment, and damage to their credit rating and reputation. As LoPucki (2003) noted, "Victims have no legal remedy for a false report if the credit-reporting agency followed 'reasonable procedures'; Federal law exempts both creditors and the credit-reporting agencies from liability for false statements about the victims of identity theft" (p. 91). Furthermore, a credit-reporting agency is obligated to reinvestigate a case only if a victim requests it. LoPucki argued that creditors and agencies exercise a chilling effect on identity theft victims "by maintaining an attitude of skepticism toward the victim's claim of identity theft and forcing the victim to take the initiative to prove it" (p. 93).

Morris (2010) charged that little research has been conducted on who commits identity theft. According to the Bureau of Justice (2011), in 2010 approximately 8.6 million U.S. households had a victim of identity theft. That figure was up 1.5% from 2005. Morris noted that even when criminals are apprehended for alleged identity theft, it is often difficult to charge them with that specific crime, given the legal burden of proof required. Morris offered an inclusive definition of identity theft that includes check fraud, plastic card fraud (credit cards, check cards, debit cards, phone cards), immigration fraud, counterfeiting, forgery, terrorism by using false or stolen information, theft of various kinds (pick-pocketing, robbery, burglary or mugging to obtain a victim's personal information), postal fraud, computer crime, telemarketing scams, and bank fraud (p. 186).

Morris (2010) studied newspaper articles about identity theft published in American newspaper articles from 1995 to 2005. He noted that most funded research reports on the topic are limited by inadequate validity, sampling, and reliability (p. 187). Morris found that incarcerated identity thieves come from both in the working and middle classes and use their employment position to perform the crime. Most of those identified as identity thieves had prior arrests; the victimized were often family and friends. Some thieves used victims' mailboxes and trash to steal identities. Their most common motivations are "to obtain and use credit (45%), to generate cash (33%), to hide their true identity (28%), and to apply for loans or to buy a vehicle (21%)" (p. 189). In the 36 published studies Morris reviewed, about half of the identity thieves used some form of computer technology to carry out the crime. Morris's findings are summarized in Table 3.

Table 3

Indicators of Identity Theft: Sophistication Levels

1. Circumstantial 17.70%	a. ID theft based on circumstance b. Opened limited number of account in victim's name c. Opportunity simply presents itself d. No evidence of major premeditation e. Little to no planning required f. Limited number of victims g. ID theft out of perceived necessity (premeditation) involved
2. General identity theft 51.00%	a. Nontechnological in nature b. Premeditated with a small number of victims c. Includes general imposter d. Focused ID theft on single victim e. Simple, with some planning (premeditation) involved f. Opportunity arises and is specifically exploited g. Minimal level of cooperation necessary h. Physical contact with outside parties to complete scam
3. Sophisticated ID theft 25.10%	a. Incorporation of computer technology b. Digital ID theft c. Also includes nontechnological rings d. Increased number of victims e. Single party hacking leading to generation of ID information f. Increased premeditation and planning necessary
4. Highly sophisticated 6.20%	a. Complex organization b. Large number of victims c. Solitary master crook (no ring, but high $$ and longevity) d. Incorporation of forging technology e. Large-scale rings f. Extensive ring operation g. National or global area of operation

Note. From Morris (2010). Used with permission.

Anderson (2006) noted that the risk of identity theft faced by consumers differs according to demographic characteristics. For example, because cash transactions are not traceable, the use of noncash transactions, such as credit and debit cards, electronic transfers, and so forth, places one at greater risk for identity theft. To the extent that access to noncash means of payment is associated with higher socioeconomic status (SES), people with higher SES will be more vulnerable to identity theft than will those of lower SES.

Anderson (2006) cited results of a 2003 FTC survey with over 4,000 adults. Participants were asked whether their credit card, checking, or savings account information had been misused and whether their personal information had been misused. Results of the study are summarized in Table 4.

Table 4

Incidence of Identity Theft

	Percentage of population	discovering victimization
Victim of	Last year	Last 5 years
Any type of identity theft	4.6 (3.8 – 5.4)	12.7 (11.4 – 14.0)
Only unauthorized credit card charges	2.2 (1.6 – 2.8)	5.2 (4.3 - 6.1)
More than unauthorized credit card charges	2.4 (1.9 – 2.9)	7.5 (6.5 – 8.5
New accounts and other fraud	1.5 (1.2 – 1.9)	4.7 (3.9 – 5.4)

Note. From Anderson (2006). Figures in parentheses are 95% confidence intervals. Used with permission.

Anderson (2006) found that respondents ages 25-54 were most likely to be victims of identity theft, followed by those ages 18-24 and then those over 75.

Public Versus Private Safety

I have been discussing the criminal misuse of PII. A related issue is how law enforcement authorities use such information, allegedly in the interests of public safety. As Simbro (2010) noted, those authorities have benefitted by the location data available from GPS-equipped mobile phones. According to Simbro, the desire of law-enforcement agencies to apply search-and-seizure laws to cell phone data has led to a reevaluation of federal legislation, including the Fourth Amendment and the Stored Communications Act. Simbro argued for a balance between the needs of law enforcement, which sometimes result in intrusions on privacy, and the need for judicial accountability.

As Gershowirt (2011) noted, defendants have been convicted of such crimes as drug dealing and child pornography based on evidence found on cell phones. According to Gershowirt, courts have generally ruled that if police have a valid reason to arrest someone and then find a cell phone in the process, they are justified in searching the contents of the phone. To illustrate the potential legal complexity of such situations, Gershowirt posed three questions regarding what happens when police arrest a suspect who has a password-protected phone:

1. Can they attempt to break the password themselves and unlock the phone without the consent of the arrestee and without a search warrant?
2. How long can police tinker with the phone in an effort to gain access to its contents?

3. If police cannot crack the password on their own, can they request or even demand that the arrestee turn over the password without violating the Miranda doctrine or the Fifth Amendment protection against self-incrimination?

(p. 1129)

Gershowirt observed that based on case law that predates the advent of cell phones, police are allowed to search any object or container that relates to the arrest. Although a search of an arrestee's physical person must be conducted as soon and as quickly as possible, searches of other items can be done after the fact and at leisure; in short, Gershowirt concluded that the law provides cell phone users little protection against search and seizure.

Much legal discussion of privacy rights has centered on interpretations of the Fourth Amendment of the U.S. Constitution. In a review of Slobogin's 2007 book, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment*, Kerr (2009) imagined the 2035 U.S. Supreme Court designing "a new Fourth Amendment that will match their civil libertarian privacy preferences" (p. 951). In *Privacy at Risk*, Slobogin cited two practices that he claimed are not currently regulated by the Fourth Amendment: public surveillance (e.g., closed-circuit television) and transactional surveillance (e.g., access to financial and telephone records). Slobogin argued that both types of surveillance should be subject to greater regulation and proposed ways that the Fourth Amendment could be applied to that end. Kerr criticized Slobogin's approach for being too complicated by requiring courts to "master the intricacies of public opinion surveys to determine public perceptions of intrusiveness" and "to generate a complex set

of Fourth Amendment rules to govern different surveillance practices" (p. 952). Regardless of the details of Slobogin's critique, however, his book is evidence of a growing concern that legal interpretation has not kept pace with technological development.

Biometrics

Clarke and Furnell's (2007) study of knowledge-based identification illustrated the difficulty of information security. They cited a survey revealing that 44% of mobile phone users do not use a personal identification number (PIN), but 81% percent of respondents agreed that there is a need for greater security of information stored on PDAs. One problem with passwords and PINs is that as technology proliferates, the number of information repositories that a given individual needs to protect increases. Faced with the prospect of memorizing numerous passwords and PINs, many consumers use the same or similar configurations for multiple accounts, thus reducing their effectiveness.

Biometrics presents an alternative security measure that requires users only to exhibit their own inherent and unique personal features: voice, eyes, fingerprints, even the shape of their hands (Alster, 2005). The term is derived from the Greek words *bio*, meaning "life," and *metric*, meaning "measure" (Ashok, Shivashankar, & Mudiraj, 2010, p. 2402). As Sonkamble, Thool, and Sonkamble (2010) noted, using biometrics ensures that information is restricted to authorized users by requiring them to be physically present when being authenticated. Sonkamble et al. summarized the strengths and weaknesses of various form of biometrics, including fingerprints, hand geometry, facial characteristics, and eyes. They noted that fingerprints, a well-established means of

identification, consist of unique ridges and valleys in one's fingertips. Even the fingerprints of identical twins are different. Fingerprint recognition systems have provided accuracy at an affordable cost in industries such as banking and are also used on passport forms. Related to fingerprints is hand geometry, which is based on the hand's shape, size of palm, and length and width of fingers. An advantage of hand geometry is that it is unaffected by environmental factors such as dry weather or dry skin.

Facial identification includes such attributes as eyes, eyebrows, nose, lips, and chin—as well as how these attributes are uniquely configured in each human face (Sonkamble et al., 2010). Sonkamble et al. noted that privacy rights create some restrictions regarding how facial images are obtained. Voice identification is based on a combination of physical and behavioral biometrics. Mouth and nasal activity along with lips movement are used to synthesize vocalizations. This form of identification is limited by the fact that speech patterns change over time due to age, medical conditions, and even emotional states. Also, as with facial recognition, voice recognition systems are limited by difficulties in obtaining vocal samples, owing to privacy concerns. An especially promising form of biometric identification is using the iris, which remains the same throughout one's life. Both left and right irises can be tested, yielding greater accuracy and specificity.

Radha and Karthikeyan (2011) described the advantages of "cancellable biometrics" (p. 118), whereby "a set of user-specific random numbers is integrated with biometric features to address the problem of privacy and security" (p. 118). This technique, called biohashing, combines something like a fingerprint with random strings of numbers to create an especially powerful biometric, one that is almost invulnerable to

attack. According to Ashok et al. (2010), an effective biometric system is characterized by five characteristics:

1. Universality. Everyone should have the characteristic.
2. Uniqueness. No two persons should have the same manifestation of the characteristic.
3. Permanence. The characteristic should be invariant over time.
4. Collectability. The characteristic should be easily and practically obtained and measured.
5. Acceptability. The public should have no strong objection to the collecting of the biometric data. (p. 2402)

Ross and Jain (2004) distinguished between unimodal and multimodal biometric systems. The former rely on a single source of information (e.g., fingerprint, face scan, etc.). The problem with unimodal systems, Ross and Jain argued, is that they are subject to "noise" (p. 1221). For example, a fingerprint marred by a scar or a voice sample altered by congestion is an example of noisy data. Unimodal systems are also limited by intraclass variations (e.g., someone with an incorrect facial pose). A preferable approach, the authors claimed, is a multimodal biometric system, in which two or more characteristics are analyzed.

Pocovinicu (2009) defined biometrics as "the science and technology used to uniquely identify individuals based on their physical, chemical, or behavioral traits" (p. 57) and gave several examples: face, fingerprints, hand geometry, iris, retinal scan, signature, voice, facial thermograph, odor, DNA, gait, ear canal. Pocovinicu listed several advantages of a biometric trait: It cannot be lost or shared, it is cost-efficient, it can

provide emergency identification, and it prevents identity theft (p. 59). Pocovinicu suggested five criteria for rating the effectiveness of a biometric system:
(a) uniqueness: how well the biometric trait separates one individual from another;
(b) permanence: how well a biometric trait resists aging; (c) collectability: ease of acquisition of the biometric trait without causing inconvenience to the user;
(d) performance: accuracy, speed, and robustness of technology used, (e) acceptability: degree of approval of the biometric technology by the user; and (f) circumvention: ease of use of an imitation of the biometric trait (p. 59). The ability of a cell phone to capture images means that some biometric traits (e.g., fingerprints, hand geography, voice) could be used to authenticate a cell phone user's identity.

Pocovinicu (2009) described how biometrics can be used with cell phones to match a voice recording to a prerecorded vocal sample in order to authenticate the phone user. Pocovinicu cited biometrics as an example of "possession-based authentification" (p. 57), as opposed to "knowledge-based authentification" (p. 57). The advance of informational technology has led, in the view of some observers, to new public attitudes toward privacy. As Roberts and Schreft (2009) noted, the fact that personal information is now much more readily available electronically suggests a need for an accounting of both the benefits and the costs of a shrinking zone of privacy.

According to Pheterson (2011), all U.S. military personnel and contractors now carry a Common Access ID Card that contains biometric data, photographs, and holograms. Pheterson argued that civilian use of such cards would simplify security efforts at borders and airports. He also cited an example of face-recognition technology whereby filmmakers can assess individual audience members' reaction to a film.

Pheterson (2011) noted several concerns about the "gathering storm of data" (p. 114) being collected by public and private entities. The first has to do with security. Pheterson cited the highly publicized WikiLeaks incident, when a U.S. military member provided classified information to WikiLeaks, which promptly released the information through its website. A second concern has to do with the authenticity of biometric data stored on cards or other portable devices. Pheterson predicted that companies that collect and use biometric data without adequately protecting their security are likely to face legal challenges.

Pheterson (2011) recounted one hopeful sign in an otherwise pessimistic account of the potential for misuse of biometric data. Google's Picasa is a cloud-based photo service that enables people to store digital images and sort them using face-recognition technology. According to Pheterson, the Picasa software is configured so that someone cannot use a smart phone to take a digital photo of a person and then use Google to search for similar faces in the vast Picasa image database. Google, apparently out of a concern for privacy, allows searching for other kinds of images but not faces.

Riley et al. (2009) studied biometric technology in India, South Africa, and the United Kingdom. The researchers found that attitudes toward biometrics varied according to cultural background. The most frequent concerns had to do with data security, health, and safety. The authors concluded that biometrics is not unique in being affected by cultural context.

Nwatu (2011) studied attitudes toward biometric identification to reduce identity fraud in Nigeria. The study was based on the technology acceptance model, which posits that technology use is influenced by utility and ease of use. Nwatu found that

participants' general awareness of biometrics technology, together with their opinions about ease of use and security, determined how they viewed the technology as a means of addressing identity fraud. Nwatu argued that biometrics represent a powerful weapon against identity fraud, which contributes to social unrest and instability.

Obstacles to Security

Crompton (2010) argued that strengthening network security through identity management must focus not just on an organization's interests but also users' interests. Stajano and Wilson (2011) agreed, warning that designing electronic security systems without considering how actual users behave is a recipe for failure. They argued that security system design must be based on the human element, and they described six obstacles to security:

1. *Distraction*. "When people are focused on what they want to do (which is most of the time), the task they care about distracts them from the task of protecting themselves" (Stajano & Wilson, 2011, p. 11). An example of distraction is the Nigerian money transfer scam, in which a purported Nigerian government official allegedly wants to transfer money out of the country. A victim who is sufficiently distracted by the prospect of unexpected financial gain can be persuaded to send money for "expenses," not realizing that the entire enterprise is fraudulent.

2. *Social compliance.* Criminals learn to exploit people's otherwise laudable respect for authority by creating bogus versions of authority. In the computer realm, a common ploy is *phishing*, which typically involves sending an e-mail from a purported systems administrator or bank official instructing the victim to visit an official-looking website and surrender personal identification information; because the e-mail and website

sound and look official, and because people are conditioned to comply with authority figures, phishing can be effective.

3. *The herd principle.* Criminals know that people will tend to do what others around them are doing. Stanjano and Wilson (2011) noted that a variety of terms have been created to describe various ways cybercriminals exploit the herd principle. *Sockpuppets* are "multiple aliases created by the same person in order to give the impression that many other people share a given opinion" (p. 14). *Astroturfing* is "the practice of introducing fake identities to simulate grassroots support for a candidate, party or idea" (p. 14). In peer-to-peer networks, *sybils* are "multiple identities controlled by the same attacker" (p. 14).

4. *The dishonesty principle.* Stanjano and Wilson (2011) observed that people who fall prey to a scam that has them doing something disreputable will, having eventually discovered the scam, often fail to report it to authorities for fear of being implicated in the disreputable activity. For example, a Trojan horse virus that infects an entire computer network might have promised users free access to pornography. Those who fall prey to the scam will be reluctant to help authorities track its origins.

5. *The deception principle.* Stanjano and Wilson (2011) noted that most computer systems security measures are based on authentification. They emphasized that not only must system administrators authenticate users but users must also authenticate computer systems; failure to do so can make one a victim of phishing. They stated that "users are very good at recognizing known people but easily deceived when asked to authenticate objects or unknown people" (p. 16).

6. *The time principle.* People behave differently when they believe they are under time pressure than when they are not. In the online world, computerized stock trading and auctions create an environment where, under the guise of limited time, people can be exploited by unscrupulous agents to make decisions they would not otherwise make (Stanjano & Wilson, 2011).

Future Trends

Many observers predict that cybercrime will continue to plague technology users, probably getting even worse than it is now. A recent article in *Trends Magazine* predicted that attacks on cell phones and PDAs will continue to grow, creating a "mix that is ripe for illegal cyberactivity" ("The Internet grows," 2011, p. 27). The article also mentioned the vulnerability of voice over Internet protocol (VoIP) to hacking.

Katzan (2011) stated that "the nation's digital infrastructure is in jeopardy because of inadequate provisions for privacy, identity, and security" (p. 1), resulting in a need for users of computer networks to act defensively. Katzan charged that individual technology users and system administrators are inadequate to the demands of cyber security and called for the intervention of a third party. Because much cybercrime originates from other countries, controlling it is an international matter.

Summary

In this chapter, I reviewed the relevant literature for a study of how cell phone use is affected by attitudes toward privacy and identify theft. The right to privacy is not explicitly addressed in the U.S. Constitution, but the courts have generally interpreted the Fourth Amendment as guaranteeing some degree of privacy. Rapid technological developments have complicated the issue of privacy because users of credit cards, ATMs,

computers, cell phones, and other PDAs—simply by virtue of using those devices—leave an electronic record, or footprint, of their activity. The use of that information by legitimate businesses and law enforcement entities has raised questions about what are appropriate uses of PII, and the obvious misuse of PII by criminal elements has generated serious concerns about the extent to which such information should be protected.

A particular form of cybercrime is identity theft, which predates the widespread use of cell phones but which is facilitated by their use, to the extent that cell phone transactions can be illegally monitored. Resisting cybercrime involves two main approaches: knowledge- and possession-based authentification. The former consists of such things as passwords and PINs, whereas the latter includes such things as voice recognition, retinal scans, DNA, and so forth. The latter is the province of biometrics—a way of identifying individuals based on their unique physical or behavioral traits.

Consumer reaction to the collection of PII has not been adequately studied. On one hand, many people seem willing to share some PII voluntarily through such web-based venues as Facebook, Twitter, and Foursquare. On the other hand, there is some evidence of a consumer backlash to the widespread collection of PII for commercial purposes. It is not known the extent to which people's fears about cybercrime constrain their use of electronic forms of communicating and transacting business. Those gaps in understanding were the focus of the current study. In Chapter 3, I will describe the study's methods, including research design, sample, data collection and analysis procedures, and steps taken for the ethical protection of participants.

Chapter 3: Methodology

Introduction

In this chapter, I will describe the methods for a study on how cell phone use is affected by attitudes toward privacy and identity theft. The focus of the study is the use of biometrics. Potential participants received an invitation letter (see Appendix A), and all participants signed an informed consent form (see Appendix B). Data collection was based on personal interviews (see Appenix C) with a convenience sample representing employees of a biometrics company and private citizen cell phone users. Data were analyzed by coding for emergent themes.

Research Design

This study was based on a qualitative design, which Glaser (2004) and Polkinghorne (2005) described as appropriate for determining what people have experienced. According to Merriam (2009), the purpose of qualitative research is to develop an understanding that is mutually experienced and mutually understood by the entities involved. Singleton and Straits (2010) observed that qualitative studies are more common in the social sciences, whereas quantitative methods dominate research in the natural sciences.

Moustakas (1994) listed several differences between quantitative and qualitative research: (a) In qualitative studies, researchers are concerned with experience as whole rather than its constituent parts, which a quantitative researcher would emphasize; (b) qualitative studies represent a search for the meaning of experience rather than an attempt to measure and classify it; and (c) in a qualitative study, the relationship between subject and object, and between the parts and the whole, is the focus of attention.

The current study was phenomenological. Robson (2002) defined a phenomenological study as "a theoretical perspective advocating the study of direct experience taken at face value; it sees behavior as determined by the phenomena of experience, rather than by external, objective and physically described reality" (p. 550). For Creswell (2007), the purpose of a phenomenological study is to describe "what all participants have in common as they experience a phenomenon" (pp. 57-58). Creswell distinguished between hermeneutic and psychological phenomenology. The former is more concerned with individual behavior and opinions, the latter with the collective significance and meaning of what people say and do. Moustakas (1994) described phenomenology as "committed to descriptions of experiences, not explanations or analyses" (p. 100). Moustakas devised a seven-step process for conducting phenomenological research:

1. Discover a topic based on "autobiographical meanings and values" (p. 103).
2. Review the literature.
3. Find appropriate coresearchers (i.e., participants).
4. Develop an informed consent form that describes the study's nature and purpose, confidentiality guarantees, and responsibilities of researcher and participants.
5. Formulate interview questions.
6. Conduct individual interviews.
7. Organize and analyze interview data. (pp. 103-104)

The other main option for this study would have been quantitative research. Such an approach would have permitted me to canvass a greater number of participants. That increased breadth, however, would have come at the expense of the depth that can be achieved with a qualitative study based on individual interviews. Because I was interested in the lived experience of people who are on the cutting edge of informational technology, a qualitative study was deemed the superior approach.

Other qualitative research designs were also considered. For example, in a grounded theory study, one purpose is to analyze and strengthen existing theories; another potential purpose is to create new theory. Grounded theory is inductive rather than deductive; that is, it emerges out of a collection of data rather than being deduced from an existing theory or framework (Robson, 2002). Another design is the case study, which Creswell (2007) described as an attempt to categorize people's reactions to a given set of conditions in a particular social setting. Related to the case study is ethnography, which typically relies on interviews and observations of people going about their daily lives (Trochim & Donnelly, 2006). Finally, a researcher can base qualitative data collection on focus groups, in which people are interviewed in groups rather than individually. The assumption behind such an approach is that the process of group interaction leads to observations and reflections that people would not make on their own. Trochim and Donnelly noted that one challenge of using focus groups is logistical: gaining access to the requisite number of people and assembling them at a particular time and place. Another test is finding a skilled facilitator(s) who can put people at ease, draw them out, and keep them on topic.

Role of the Researcher

As is the case with much qualitative research, in the current study I was the primary means of data collection. I personally conducted all the individual interviews. To perform my role with maximum objectivity, it was necessary for me to set aside any preconceived notions about the topic at hand, a process that is called bracketing or epoché. Bracketing involves setting aside previous experiences or current opinions that might compromise a researcher's objectivity in attending to or interpreting a given phenomenon (Bednall, 2006). The process is facilitated by what Bednall (2006) called a *feelings audit*: listing personal values and dispositions that might affect a researcher's observation of and response to others.

Research Questions

This study was based on three research questions:

1. To what extent do biometrics industry representatives and cell phone users connect cell phone use with decreasing privacy and identity theft?
2. How is cell phone users' behavior affected by their attitudes toward privacy and identity theft?
3. What steps can be taken to reduce the incidence of identity theft associated with cell phone use?

These questions were used to inform a set of semistructured interview questions (see Appendix C).

Ethical Protections

In keeping with Walden University requirements for research involving human subjects, permission to conduct the study was obtained from Walden's Institutional

Review Board (approval #03-21-13-0018283) and from the company that furnished some interviewees (see Appendix D). All participants signed an informed consent form (see Appendix B) that describes the study's purpose and benefits, states the voluntary nature of participation, assures confidentiality, and describes procedures for member checking and obtaining a summary of the study's results. In all written descriptions of the research, participants are referred to by number. No individual names, company or agency names, or other identifying information are used in any written report. Interview data, both paper copies and electronic files, will be kept in a locked office and on a password-protected computer accessible only to me. Data will be kept for 5 years, at which time they will be destroyed.

Population and Sampling

In phenomenological studies, it is necessary that participants have experience with the phenomenon under investigation. I used purposive sampling, a process Creswell (2005) described as selecting individuals who have experience or qualifications with the phenomenon under investigation. I selected 30 participants representing three groups: (a) a biometrics company from the private sector, (b) individual cell phone users with annual salaries over $55,000, and (c) individual cell phone users with annual salaries under $55,000. A sample size of 30 is within the range recommended for a study based on individual interviews (Creswell, 2005). I targeted one private sector company and interviewed 11 employees from it. I also interviewed 19 private citizens who were cell phone users. Interview questions were informed by the research questions. A list of interview questions appears in Appendix C.

Potential participants received an invitation letter that described the study's purpose and methods (see Appendix A). They were instructed to reply by e-mail or phone if they were interested in participating. Individual interview appointments were scheduled by phone. Participants received a copy of the consent form in advance of the interview (see Appendix B), which was signed before an interview began.

Data Collection Procedures

The primary means of data collection was individual, face-to-face interviews. Interviews were conducted at a mutually convenient location and were audio recorded. An interview protocol was used (see Appendix C). The interview protocol was based on Rubin and Rubin's (2005) recommendations. Rubin and Rubin stressed the importance of an interviewer establishing a comfortable and welcoming atmosphere, refraining from imposing his or her own perspectives or opinions on the exchange, and being flexible in reacting and adapting to interviewees' responses. Rubin and Rubin also recommended leaving sufficient time after an interview to summarize the researcher's impressions and any notes taken during the interview itself. All participants signed an informed consent form that explained the nature and purpose of the study, assured anonymity and confidentiality of all responses to interview questions, and made it clear that they could withdraw from the study at any time without penalty, or refuse to answer any questions with which they were uncomfortable (see Appendix B).

Interviews were based on questions outlined in Appendix C. Questions were designed to elicit respondents' descriptions of their personal and professional experience with privacy, security, and inappropriate or criminal activity associated with cell phone use. Interviews lasted 40-60 minutes. Interviews were semistructured; that is, all

interviewees in a given group were asked the same questions, but follow-up questions varied by individual. Before beginning an interview, I engaged in brief, casual conversation with the interviewee to create a relaxed, nonthreatening atmosphere. This approach is in keeping with King and Horrocks's (2010) emphasis on the importance of the relationship between interviewer and interviewee in a qualitative study.

Validity and Reliability

Although considerations of validity and reliability are usually applied to quantitative research, Maxwell (2004) argued that they are also important in qualitative studies. Creswell (2007) described several strategies for enhancing validity in qualitative research, including triangulation, peer review, and member checking. Triangulation involves collecting data from a variety of participants and settings (Maxwell, 2004), which was accomplished in the current study by interviewing people from three groups. Member checking was accomplished by giving participants an opportunity to review their interview transcripts for accuracy.

Data Analysis

Data analysis began with a transcription of each interview. Transcriptions were done by a professional transcriber. Data analysis was undertaken in the manner described by Moustakas (1994) as epoché, or bracketing: "the suspension of everything that interferes with fresh vision" (p. 86). In coding, I followed the general procedures outlined by Berkowitz (1997), who suggested six questions to ask:

1. What common themes emerge in responses about specific topics? How do any patterns illuminate the research questions or hypotheses?

2. What might explain any deviations from the patterns that have been noted?
3. How might participants' environment or previous experience affect their behavior or attitudes?
4. How do respondents' stories illuminate the research questions?
5. Do particular responses suggest the need for additional data?
6. How do the patterns observed compare to the results of other studies on similar topics?

Coding of data was accomplished by use of NVivo software, designed to facilitate organizing and analyzing nonnumerical data. According to the manufacturer, QSR International, NVivo is useful for analyzing survey responses and includes sophisticated text-analysis features. The software allows a researcher to create visual representations of the data, such as word trees and connections maps (QSR International, 2012) A list of themes generated by NVivo can be found in Appendix E.

Summary

In this chapter, I discussed the methods for a qualitative study of how cell phone use is affected by privacy, security, and cybercrime. Data collection was based on in-person, semistructured interviews of representatives from three groups: employees of a biometrics company, individual cell phone users with annual salaries over $55,000, and individual cell phone users with annual salaries under $55,000. Interviews were transcribed and coded for themes. Data analysis was conducted using NVivo software. Special attention was given to handling all personal data in order that the identity of any

participant would be impossible to determine. In Chapter 4, I will describe the results of the study.

Chapter 4: Results

In this chapter, I will summarize the results of a phenomenological study designed to determine participants' attitudes toward privacy and identity theft in relation to cell phone use. The study was based on 30 individual, semistructured interviews with biometrics industry representatives and individual cell phone users. Interviews were conducted between September 2013 and October 2012; they lasted 40-60 minutes each. Interviews were conducted at locations convenient for participants. Interviews were transcribed and analyzed for themes.

Overview of Study

I conducted this study because identity theft has emerged as the most frequent consumer complaint in the United States. In 2010, over 250,000 such complaints were received by the Federal Trade Commission's Consumer Sentinel Network. At 19%, that category represented by far the largest of those maintained by that agency (FTCCST, 2011). Accompanying the rise in identity theft has been an increase in cell phone use. Cell phone subscriptions increased from 97 million in 2000 to over 331 million at the beginning of 2012 (CTIA, 2012). Because cell phones are increasingly used to store a wide variety of personal information, their owners are vulnerable to identity theft and a loss of privacy if a phone is lost or hacked. Whether that possibility affects cell phone users' attitudes has not been studied, and that gap in the literature is what gave rise to the current study.

This study was phenomenological. The purpose of a phenomenological study is to describe "what all participants have in common as they experience a phenomenon" (Creswell, 2007, pp. 57-58). Phenomenological research is more descriptive than

analytical (Moustakas, 1994). The phenomena under investigation in the current study were cell phone use, identity theft, and loss of privacy.

Data Collection and Analysis Procedures

Data collection was based on individual interviews. Participants represented three groups: employees of a biometrics company, private citizens owning cell phones and earning less than $55,000 annually, and cell phone owners earning more than $55,000 a year. I interviewed 11 biometrics employees and a total of 19 individual cell phone users. Interviews were semistructured in that each participant was asked the same set of questions, with individualized follow-up questions used as appropriate. Interviews were transcribed and analyzed for themes.

Demographic Information

Participants were asked to supply demographic information: age, gender, ethnicity, and annual income. This information is summarized in Table 5.

Table 5

Demographic Information for Sample

Participant	Gender	Ethnicity	Age	Income
1	Male	African American	>55	>$100K
2	Male	African American	>55	>$100K
3	Male	African American	18-30	$56-$65K
4	Male	European American	18-30	$ 66K-$75K
5	Male	European American	31-40	$76K-$100K
6	Female	European American	31-40	$76K-$100
7	Male	European American	31-40	$66K-$75K
8	Female	European American	31-40	$30K-$50K
9	Female	East India/Spain	31-40	$30K-50K
10	Male	European American	31-40	$66K-$75K
11	Female	East India/Spain	31-40	$56K-$65K
12	Male	East India/Spain	41-55	$66K-$75K
13	Male	European American	41-55	$76-$100K
14	Male	European American	>55	>$100K
15	Male	African American	41-55	>$100K
16	Male	African American	18-30	$51-$65K
17	Female	East India/Spain	31-40	$51-$65K
18	Male	African American	41-55	$76-$100K
19	Female	African American	31-40	$66K-$75K
20	Male	African American	>55	>$100K
21	Female	African American	41-55	$76-$100K
22	Male	African American	>55	>$100K
23	Male	African American	31-40	$56K-$65K
24	Female	African American	31-40	$76-$100K
25	Male	African American	31-40	$76-$100K
26	Female	African American	41-55	>$100K
27	Male	African American	41-55	$56-$65K
28	Male	African American	31-40	$35K-$50K
29	Female	African American	31-40	$35K-$50K
30	Female	East India/Spain	31-40	$35-$50K

Interview Data

Participant 1

Participant 1 was a retired United States Air Force (USAF) officer who spent 22 years with the USAF. He also had been a consultant and owned his own business. Since retiring, he has spent most of his time travelling with his wife and supporting his church and organizations in his community.

He stated that cell phones contribute to identity theft and emphasized that personal information should not be stored on a cell phone and that personal identification numbers should be used for security. He received several unsolicited text messages per week and deleted them immediately. He was cautious about blogging and said it should not be done on a cell phone.

Participant 2

Participant 2 is retired from Hewlett Packet, having worked in the field of information technology for more than 30 years. He kept his cell phone on at all times. He noted that cell phones make people reachable all the time, making each person in effect a virtual office. He said that if a cell phone is stolen, the information stored on it can be easily stolen if there is no password. To reduce or eliminate identity theft, he said that identity verification should be required for all applications for credit. Nevertheless, the best protection from identity theft is taking care to ensure all personal information is protected. He said that biometrics technology has had a positive effect on protecting individuals from identity theft. He gave the example of requiring a fingerprint before accessing information from a smart phone.

Participant 3

Participant 3 was a high school teacher. He urged caution about keeping online passwords for cell phones and expressed concern about the susceptibility of government entities to cyber attacks. He recommended the use of retina-reading devices to check the identity of a cell phone user.

This participant used a variety of social media: Facebook, Instragram, Twitter, Circles, Google+, and LinkedIn. He had been a target of phishing. He did not blog even though he does manage a website. He believed that biometrics will help prevent identity theft because biometric data cannot be stolen or duplicated.

Participant 4

Participant 4 expressed concerned about leaving cell phones at home or in a car, where they would be subject to theft. He said that because most cell phone calls are not secured or encrypted, the information transmitted could be captured by a third party. He lamented that most people probably do not consider the security implications of entering credit card or Social Security number information via a phone. Capturing cell phone transmissions could yield a great deal of information, though he acknowledged that such information might not be targeted; that is, it would be harder to track John Doe's information than to capture *someone's* information.

To improve cell phone security, Participant 4 recommended encryption, spread spectrum, and frequency hopping. He also said that people should reduce their information footprint as much as possible by not providing any more information than is required in online transactions. He noted that widespread data mining by government and private industry means that others have information about a person that the person might

not even know him or herself. He said that with identity theft, “If you have multiple people running around claiming to be you, you can no longer ensure that you did or did not perform any particular action.” Participant 4 also noted,

> The fact nearly every move you make is tracked, recorded, or otherwise monitored means that to be completely safe, you would have to move to an off-grid log cabin in the mountains to avoid tracing. Even then, the Wal-Mart where you buy groceries or the gas station would likely be issues. If you are truly paranoid, use cash and ride a bike (new cars can be tracked). Oh, and wear a veil.

Participant 5

Participant 5 was the subject of identity theft in 1992 when he received a phone call from a department store detective informing him that his company credit card was maxed out. He offered several suggestions for reducing identity theft: (a) shred credit card offers, (b) use point-of-sale terminals with keypads to confirm credit instead of giving a card to someone, (c) use aliases whenever possible, (d) use a service such as Identity Guard, (e) pay attention to credit reports. (f) opt out of data mining websites, and (g) limit the amount of personal information a person provides on social media.

Participant 6

Participant 6 said that identity theft increases as technology advances. She recommended more security devices for cell phones and additional education about how to prevent ID theft. She received unsolicited text messages about once a month—usually sales-oriented.

Participant 7

Participant 7 called identity theft "a problem for democracy more than for me personally." He said that the public at large is mostly ignorant about the threat of identity theft. In his industry, on the other hand, many steps have been taken to educate employees and protect them from identity theft. Participant 7 stated,

> Personal devices at work save money for the corporation, so they are driven to enable access to corporation data, applications, collaborative tools, and e-mail via personal cell phones. To avoid security problems, we use centralized cellular management systems to control data, wipe phones remotely, and compartmentalize data.

He said that no one's electronic communication is private and added that identity theft will continue to be a problem if people "treat the cell phone as an appliance and trust software vendors and telecoms to protect them." He concluded that we should "use technology to fight technological problems. It's easier than attempting to manipulate behavior."

Asked whether using a cell phone makes one vulnerable to identity theft, Participant 7 replied,

> I don't use it to make transactions and don't keep passwords on it. If the criminals (or anyone else) penetrated my phone apps, they could try to move money or open accounts. But they can do that without my phone. The phone is just another computer.

To reduce identity theft, he recommended using firewalls, passwords, and encryption; avoiding cell-phone-based bank transitions; and more thorough vetting of identity by banks, Internet institutions, and credit card companies.

Participant 8

Participant 8 said that the rise of identity theft is because smart phones can be hacked more easily than computers. To address the problem, she recommended adding security features such as data encryption and using a device similar to Lojack on digital media "to render it unusable if an unauthorized user happens to access your device."

Participant 8 said she does not blog and accesses the Internet from a PC, not from a cell phone. She once lost her cell phone but was able to disconnect it immediately. She said that personal information should not be kept in cell phone databases, but if it is it should be encrypted.

Participant 9

Participant 9 said that although using a cell phone enables outsiders to track where one is and who one is talking to, the public at large does not connect this capability to identity theft. Participant 9 claimed, "Losing your cell phone or getting it hacked is a big concern." To protect oneself, she recommended not storing personal information on a phone and having an unlisted number. Despite a person's best efforts, however, "if somebody hacks Amazon's website and steals information, how can I prevent that?"

Participant 10

Participant 10 said there was no longer any widespread expectation of privacy—neither on the job nor as a private citizen:

The courts have effectively ruled that by carrying a cell phone and having that phone turned on, a person essentially waves their Fourth Amendment right. There are competing court rulings, but for now it seems that an individual cannot expect privacy.

He said that cell phones uses make it easier to commit identity theft because of the personal information stored on them: user IDs, passwords, account information, and so forth. He added that many people do not use passwords or timeout features on their phones. Also, text messages can be captured.

To reduce or eliminate identity theft, he recommended that companies not allow bring your own device (BYOD). “Allowing personnel devices to connect to corporate networks can expose that network and related data. If a company allows BOYD, policies and technologies must be put in place to limit exposure to company assets.”

To prevent identity theft,

- Do not store personal information on your mobile devices.
- Check your financial accounts frequently. Set up automatic alerts to notify you when specific activity is performed on an account.
- Set up access passwords on your mobile devices and have them automatically lock when a given time limit is exceeded.
- Have a way to wipe the mobile device if a password is entered incorrectly after too many times and/or remotely enable a wipe of the device.
- Do not share personal information on social sites. Lock them down to limit public access.
- Set up automatic security defaults on mobile (and nonmobile) devices.

- Set all standing data (data at rest) to be encrypted. Ensure people have to opt out of security on social networking sites rather than having to set up security.

Participant 11

According to Participant 11,

With the arrival of smart phones, e-mails, passwords, and other personal information is at risk. A way to make cell phones more secure is to have mandatory and secure access codes, remote wire capabilities, and handling guidelines. Additionally, those that utilize cell phones should be aware of surroundings, know basic security measures, and maintain secure and unique passwords.

Participant 11 used Facebook, Linkedln, and Google+. She said that although biometrics has helped reduce identity theft, it can also " promote a false sense of security and decrease vigilance."

Participant 12

Participant 12 said, "I assume if a cell phone is lost, then the information in that device can be retrieved and used for identity theft." To minimize that threat, he recommended encrypting phones, equipping them with passwords, and limiting personal information stored on them. In addition, it should be possible to wipe a cell phone remotely.

Participant 13

This participant managed a website, had never lost his cell phone, and had antitheft measures installed on his phone. He said the organization where he worked was

not affected by identity theft, but in organizations where stealing an employee's identity could provide a great reward, it would be a problem. He said people who not understand the basics of security are most at risk. He recommended not storing sensitive data on a cell phone.

Participant 14

This participant believed that identity theft was a big problem in the travel industry and that cell phone use had exacerbated the problem. To improve security, he recommended several measures: using GPS Tracer, requiring an ID and password (or fingerprint) to access a phone, configuring the phone to lock after a specified period of nonuse. Participant 14 said he had been a target of phishing only once, had never lost his cell phone, and used Safe Guard PII.

Participant 15

Participant 15 was a software engineer specializing in cyber security. He noted that sensitive information falling into the wrong hands could threaten an organization. To make cell phones more secure, he recommended implementing a comprehensive information security program. He said that information theft is a problem that is here to stay, so professional expertise must be strengthened, including the use of biometrics.

Participant 16

Participant 16 said that people in his company are not allowed to use cell phones on the job. He lamented the fact that many people store all manner of sensitive information on their phones without safeguarding it. To reduce identity theft, he recommended providing more training for employees, being careful what one posts on social media, and strengthening passwords. He said, "Data security is very important in

this digital age, because everything is moving into a technology capability, whether it be phones, cars, homes, online banking, or payroll."

Participant 17

Participant 17 said that protecting privacy in her industry would be aided by blocking incoming e-mails that are not work-related. She said that storing personal information on one's phone and accessing banking sites from a phone make one more vulnerable to identity theft. She used her cell phone only to make personal calls, and "none of the numbers I call are of interest to other people." She attributed most identity theft to ignorance on the part of cell phone users.

Participant 18

Participant 18 said that identity theft is a moderate problem in industry but a serious problem in the public at large. He recommended greater use of encryption and specialized software to deter unauthorized access and identity theft. He lost a cell phone twice and was notified by his bank of unauthorized purchases. He said that biometrics represent one of the strongest safeguards against unauthorized access of cell phones.

Participant 19

Participant 19 said that work e-mail sent to a personal phone could be a security risk but added that she is not aware of any problems with identity theft in her workplace. She cited mobile banking apps as a contributor to identity theft. She recommended requiring fingerprint ID to access phones and having the capability to deactivate a phone remotely.

Participant 20

Participant 20 said that cell phone security in his workplace is adequate but stated that it is problematic in some industries and prevalent among the public at large. He recommended installing better electronic antitheft programs, improving firewalls, and stiffening penalties for unauthorized use of information. He noted that identity theft represents not only a threat to one's financial standing but also to one's reputation.

Participant 21

Participant 21 characterized identity theft as a serious problem both in industry and among private citizens. She recommended changing passwords frequently and using voice recognition software.

Participant 22

Participant 22 said cell phones have changed the employee-boss relationship because employees are now always on call and their privacy has been invaded. She recommended imposing more stringent controls on whom in an organization has access to sensitive data and using face recognition and encryption.

Participant 23

Participant 23 recommended confining one's use of a cell phone to communication with trusted users—friends and relatives.

Participant 24

Participant 24 described identity theft as a serious problem both for industry and private citizens. She had been the target of identity theft, which she learned of through her bank. She said relying on electronic antitheft measures, including biometrics, is short-sighted because it creates a false sense of security.

Participant 25

Participant 25 said the use of firewalls and the segregation of personal data from company data has made information secure in his industry. However, in the public at large there is a significant problem. He stated that the software is only as good as the policies that ensure proper cell phone use. His e-mail account was once hacked, which he learned about from friends who received an unauthorized e-mail message purportedly from him. He expressed confidence in biometrics to reduce identity theft but said such measures are still not widely used.

Participant 26

Participant 26, a government employee, regularly handles confidential and sensitive information. She said that using cell phone could increase the chance that such information might be misappropriated. She recommended that people not divulge their Social Security number or other personal information over the phone. Her own cell phone use is confined to safety issues: "911, AAA, letting people know I have reached my destination safely or that I'm running late, and so forth." Regarding the effect of biometrics on protection against identity theft, she said,

> It is positive in some ways due to fast and convenient tools to communicate with other people and send information. However, there can be drawbacks when you are not mindful of own dissemination of personal information. Additionally, some tools cause people to be distracted, especially in public places, walking on streets, driving, conversing attentively.

Participant 27

This participant was critical of BYOD policies, stating that they contribute to a loss of privacy as well increasing the chances for identity theft. To reduce that threat, he suggested using a mobile device management system, using bio-based authentication (e.g., fingerprint), limiting the information provided through social networking, and encrypting data. He predicted that data security efforts will continue to increase and that privacy will continue to decrease. He was a victim of identity theft, which he learned about from a credit reporting agency.

Participant 28

Participant 28 downplayed the role of cell phones in contributing to identity theft, observing that "there are more wallets stolen than cell phones." He acknowledged, however, that divulging personal information over the phone, such as credit card or Social Security numbers, leaves one more vulnerable to identity theft. He sees biometrics as a possible threat to security "because these industries are constantly placing personal information on the Web."

Participant 29

Participant said that "as long as there are computers and cell phones, someone will find ways of theft." She was a target of identity theft once and learned about it by a credit check.

Participant 30

Participant 30 said that a major problem with cell phone use is that most passwords are weak. She said that cell phone use contributes to a loss of privacy as well as increasing the possibility of identity theft.

Themes by Interview Question

Interview transcripts were imported into NVivo 10, a qualitative analysis program (see Appendix E). Results of that analysis are presented by interview question. References to groups are as follows:

Group 1: employees of a biometrics company

Group 2: individual cell phone users with annual income over $55,000

Group 3: individual cell phone users with annual income under $55,000

Interview Question 1

How does cell phone use affect individual and organizational privacy in your industry? In other industries?

Interviewees interpreted this question in both personal and organizational terms. Personally, they pointed to the fact that the ubiquitous presence of cell phones has created the expectation that everyone will be "on call" around the clock. As one participant noted, this expectation means that the cell phone constitutes a "virtual office" for any employee. Individual privacy, then, is threatened by the likelihood that even when one is away from the workplace, one will be confronted with business-related concerns.

An organizational manifestation of how cell phones affect privacy has to do with how they are typically used. Unlike a land line, which confines one to an office, a cell phone can be used anywhere. Because an employee might use a cell phone in a public place to conduct a business-related call, the possibility exists that sensitive information could be overheard. In such an instance, the organization's privacy is breached.

Interview Question 2

To what extent is identity theft a problem in your industry? In other industries? Among the public at large?

Only six interviewees identified identity theft as a significant problem in their industry. Among these, the consequences of identity theft were as likely to be seen as personal as they were to be considered in organizational terms. Several participants noted, for example, that identity theft could destroy one's personal credit rating.

A majority of interviewees considered identity theft to be a problem among the public at large. They attributed this problem to the fact that in the workplace, people are educated about security measures, whereas the typical citizen may not be. Several participants characterized most citizens as careless about security. One lamented the prevalence of what he called "poor phone hygiene." Several warned about the dangers of divulging personal information such as credit card or Social Security numbers over the phone.

Interview Question 3

How does cell phone use contribute to identity theft?

Several participants cited the ease of hacking a cell phone as a major contribution to identity theft. They also mentioned people's tendency to give sensitive information over the phone. An observation made by many interviewees is that because cell phones are mobile devices, they are much more likely to be lost or stolen than are other repositories of personal information, such as PCs. If a lost or stolen cell phone is not protected by password, fingerprint or voice recognition, or some other security measure, its contents are open to whoever finds or steals it.

Interview Question 4

What could be done within your industry to make cell phone use more secure?

The most common response to this question was to institute measures such as passwords, security codes, and voice or fingerprint recognition. Another frequent suggestion was to encrypt all cell phone transmissions. Behavioral changes were also mentioned, such as limiting the amount of personal information stored on a cell phone. In general, though, the sentiment expressed by one interviewee was representative: "Use technology to fight technological problems. It's easier than attempting to manipulate behavior."

Interview Question 5

What other steps would reduce the incidence of identity theft?

Here participants mentioned several steps: instituting a time-out feature on phones, enabling remote shutdown and wiping of a phone's contents, changing passwords frequently, refusing to give credit card numbers to people one does not know.

Interview Question 6

What other thoughts do you have about data security in a digital age?

Several interviewees expressed the opinion that data security will continue to be a serious problem. As one of them put it, "Information compromise is here to stay, so professional expertise must be strengthened." Another said, "The government, both the U.S. and foreign, is using information stored and transmitted on the Internet to obtain ever more private information on individuals and groups." Another claimed that "thieves are always steps ahead of security professionals." One described the situation as hopeless: "You would have to give up every piece of digital capability in your life and

move to an off-grid log cabin in the mountains to avoid tracing." One interviewee distinguished between personal security and what might be called cultural security: "This is a problem for a democracy more than a problem for me personally, not because of the data but because of the mindset. It is a slippery slope."

Interview Question 7

How often do you receive unsolicited text messages?

Responses varied considerably, from daily to not at all. The majority of participants said they seldom or never receive unsolicited text messages.

Interview Question 8

What social networking sites do you access from your cell phone?

The majority of respondents said they access Facebook from their cell phone. Other sites mentioned were LinkedIn, Instagram, and Google+. A substantial minority said they never use a cell phone to access social networking sites. Reasons varied, from concerns for safety to the conviction that social networking is "a waste of time."

Interview Question 9

How often do you receive requests for personal information from social networking sites or other websites?

Most participants said they seldom or never receive such requests, and if they do, they ignore them.

Interview Question 10

How often have you been the target of phishing?

About half of the interviewees said they had been the target of phishing. Frequency ranged from once or twice to several times a week.

Interview Question 11

Do you blog?

Only four respondents answered this question affirmatively. One confirmed nonblogger dismissed the whole enterprise: “No. Blogging is graffiti with punctuation. I write; I don’t blog.”

Interview Question 12

Do you have your own website? Do you manage your own website?

Two participants said they have their own website, and five said they manage a site for others.

Interview Question 13

Have you ever lost your cell phone? If so, do you think information was taken from it and used to target you for identity theft? How did or would you know? What are the implications/ramifications/possible results of identity theft?

Only six participants said they had lost a cell phone. None feared that any personal information was taken from the phone.

Interview Question 14

Have you ever been the target of identity theft?

Seven participants said they had been the target of identity theft; none of those attempts were successful.

Interview Question 15

How did you learn about the theft?

Several respondents said they discovered they had been the victim of identity theft after receiving a credit report. Others were contacted by their bank or credit card company.

Interview Question 16

Does using your cell phone in the way you do make you vulnerable to identity theft?

Seven interviewees answered this question affirmatively. One said, "Social networking sites can expose personal information that can be exploited to enable identity theft." Several others said that despite their efforts, a committed hacker could probably crack whatever security measures they had instituted.

Among those who denied that their cell phone use exposes them to identity theft, several participants said that they do not store sensitive information on their phone. Others cited password or fingerprint protection as adequate measures to prevent theft of personal data, and some said they never give out credit card numbers over the phone. One interviewee, reflecting current fears about government monitoring of cell phone use, said, "I'm not aware of anything, unless the NSA is exploiting my conversations with banks or creditors."

Interview Question 17

What can be done to reduce or eliminate identity theft?

Two interviewees expressed pessimism that identity theft can be eliminated. One said, "As long as electronics are relied on, nothing can be done." Others were more sanguine. The most common suggestion was increased education about sensible cell

phone use. A representative response was as follows: “I believe that most of the time, ignorance is the most important reason for identity theft.”

Participants suggested both behavioral and technological changes. For example, “Do not provide your Social Security or credit card number over the phone.” Or, “Institute mandatory encryption and password protection.” Several appealed for tighter government regulation.

Interview Question 18

Do you think that the biometrics industry has influenced (negatively or positively) your privacy and the protection against identity theft?

Three participants said the biometrics industry has had no effect on protecting them from identity theft. Several warned of negative effects. One said, “It could promote a false sense of security and decrease vigilance.” Another said that using biometric tools could be a source of distraction if one were driving.

The majority of interviewees, however, said the influence of the biometrics has been positive. They cited fingerprints and voice recognition as data that cannot be lost or stolen. One worried, however, that such capabilities are not widely used.

Themes by Research Question

This study was based on three research questions:

1. To what extent do biometrics industry representatives and individual cell phone users connect cell phone use with decreasing privacy and identity theft?
2. How is cell phone users’ behavior affected by their attitudes toward privacy and identity theft?

3. What steps can be taken to reduce the incidence of identity theft associated with cell phone use?

In this section, I will summarize the study's major themes according to these questions.

Research Question 1

Because a cell phone is a telephone, its use involves traditional telephonic activities: placing and receiving calls to and from other individuals. In this context, participants in the current study described loss of privacy as being increased by the fact that, unlike traditional land lines, cell phones are often used in public places, where the user's part of a phone conversation might be overheard. A lack of privacy might be fairly benign, depending on the content of the telephonic exchange. However, if one is relaying sensitive personal information, having someone overhear the conversation could be more deleterious. For example, if someone else heard a cell phone user give his or her Social Security number to a person on the other end of the conversation, the risk of identity theft would be greatly increased.

But cell phones are more than just phones. They are also used to store a variety of information, some of it personal and some of it subject to misuse in the wrong hands. So-called smart phones are actually computers, and as such are subject to exploitation by hackers, as are other computers. Participants in this study expressed concern about the possibility of have a cell phone hacked, with the likelihood of this leading to identity theft. Added to the danger posed by hackers is the fact that a cell phone, being small and transportable, is subject to being lost or stolen.

Research Question 2

Participants described their cell phone use as being affected by both characteristics of the phone: its transportability and its versatility. Most interviewees were sensitive to the danger of giving out personal information (e.g., Social Security or credit card numbers) over the phone if there were a chance the conversation could be overheard. They also described a variety of steps to guard against misappropriation of personal information in the event a phone were lost or stolen (e.g., encryption, passwords, voice or fingerprint recognition).

Regarding the cell phone's use as a computer, most participants did not seem concerned about any danger resulting from using a phone to access the Internet, including social networking sites. They cited the ability to control privacy settings on such sites as adequate protection. Interviewees did not address another aspect of computer privacy that has come in for considerable discussion in other circles, namely the collection of browsing history by entities interested in using that information for targeted marketing.

Research Question 3

Interviewees described two kinds of steps to reduce the incidence of identity theft associated with cell phone use. The first was individual behavior, including such things as not using a phone where a conversation could be overheard, not leaving a cell phone unattended, not giving out sensitive information over the phone, and not storing sensitive information on a cell phone. The second category was technological steps that cell phone users can take to reduce identity theft, such as changing passwords frequently, using additional protective features such as voice or fingerprint recognition, installing a time-out feature, and enabling remote shutdown and content wiping of a lost or stolen phone.

Summary

In this chapter, I summarized the results of a qualitative study designed to determine the effect of cell phone use on attitudes toward security and identity theft. Thirty individual, semistructured interviews were conducted with people representing three groups: employees of a biometrics company, individual cell phone users earning more than $55,000 annually, and users earning less than $55,000 a year.

Interviewees were more likely to see identity theft as a problem among the public at large than in the industries where they worked. They were more worried about lost or stolen cell phones being subject to misappropriation of personal information than they were about someone hacking a phone in the owner's possession. Participants recommended a variety of measures to improve cell phone security and to reduce the likelihood of identity theft: passwords, security codes, voice or fingerprint recognition, and encryption. They tended to agree that the threat of identity theft will only increase in the future. In the next chapter, I will offer interpretations of the results and suggestions for further research.

Chapter 5: Discussion, Conclusions, and Recommendations

In this chapter, I will discuss the results of a qualitative study designed to determine the effect of cell phone use on attitudes toward security and identity theft. Data collection was based on 30 individual, semistructured interviews with participants representing three groups: employees of a biometrics company, individual cell phone users earning more than $55,000 annually, and users earning less than $55,000 a year. Interviews were transcribed and analyzed with NVivo software.

Summary of Results

Participants in this study generally agreed that identity theft is a problem that has been exacerbated by increased cell phone use. For the most part, they did not see this problem as acute in their own workplaces, where they described a variety of measures that have been taken to protect proprietary information. They were more likely to describe identity theft as problem among members of the public at large.

Regarding the misappropriation of data stored on a cell phone, interviewees were more concerned about the possibility of losing a phone or having it stolen than they were about a hacker gaining access to a phone's contents. They expressed pessimism about government attempts to reduce identity theft and stressed personal accountability. They described several things cell phone users can do to protect themselves: avoid using the phone in a public place, refuse to divulge personal information over the phone, use passwords and various biometrics (e.g., voice and fingerprint recognition), and enable remote shutoff and content wiping.

Discussion of Results

This study was prompted by an increase in concerns about privacy and identity theft generated by the growing use of cell phones. According to the Pew Research Center (2013), between 2000 and 2012, mobile phone use increased by over 300%, and in 2012 91% of U.S. adults own a cell phone, making it "the most quickly adopted consumer technology in the history of the world" (para 2). This growth in cell phone use has been paralleled by increasing concerns about cybercrime and loss of privacy. People's attitudes toward privacy are complex and sometimes contradictory (Brandimarte, Acquisti, & Loewenstein, 2013). To determine how those attitudes are influenced by cell phone use, I interviewed people about their cell phone habits. Interviews were transcribed and analyzed for themes. The following discussion is organized by research question. Three such questions guided the study.

Research Question 1

To what extent do biometrics industry representatives and individual cell phone users connect cell phone use with decreasing privacy and identity theft?

Interviewees' opinions about how cell phone use affects privacy and identity theft can be divided between what might be called active and passive behavior. On the active side, mobile technology has changed when, where, and for what people use phones. Because people carry cell phones with them, they often use the devices in public settings. This behavior affects the privacy of the user, the person he or she is calling, and those within earshot of the caller. For the latter group, the intrusion on their privacy of an overhead phone conversation is likely at worst an annoyance. For those engaging in the conversation, however, the fact that others can hear one side of it could compromise their

personal privacy in more consequential ways, depending on the nature and topic of conversation. Several participants warned about the danger of divulging sensitive information over the phone when it might be overheard—and misused—by others.

Regarding passive behavior, several participants suggested that cell phones unprotected by some security device (e.g., password, voice or fingerprint recognition, encryption) are vulnerable to exploitation by hackers. Implicit in this observation is the assumption that cell phones are more susceptible to hacking than are those connected to land lines, but none of the interviewees made this explicit comparison. More troubling than hackers, though, was the threat that personal information could be misappropriated if a cell phone were lost or stolen. Here the difference between cell phones and traditional ones is obvious: A land line phone is not likely to be lost.

Research Question 2

How is cell phone users' behavior affected by their attitudes toward privacy and identity theft?

Several interviewees said they do not store personal information on their cell phones, and a substantial majority said they do not give out sensitive information such as Social Security or credit card numbers over the phone. The majority of participants used a cell phone to access social networking sites, but in general they did not see such use as dangerous as long as reasonable privacy settings were maintained. Only one respondent said that social networking sites exposed personal information that could make one vulnerable to identity theft. Although interviewees were not asked what security measures they personally had instituted, their suggestions about encryption, passwords, fingerprint recognition, and the like imply that these were in use among many of them.

Research Question 3

What steps can be taken to reduce the incidence of identity theft associated with cell phone use?

Based on the results of this study, identity theft associated with cell phone use can be reduced by both behavioral and technological changes. Behaviorally, cell phone users can do the following:

- Avoid using a cell phone where a conversation could be overheard.
- Keep the cell phone on one's person at all times.
- Do not give out sensitive information such as Social Security or credit card numbers over the phone.
- Limit the amount of personal information stored on a cell phone.

In addition to doing or not doing certain things, cell phone users can use a variety of technological means to reduce identity theft:

- Use a password and change it periodically.
- Use a biometric protection device such as fingerprint or voice recognition.
- Install a time-out feature on the phone.
- Enable remote shutdown and content wiping of a lost or stolen phone.

Research Groups

My sample was divided into three groups: employees of a biometrics company (n = 11), individual cell phone users earning more than $55,000 annually ($n$ = 16), and users earning less than $55,000 a year ($n$ = 3). The reason for dividing the sample this way was to see if either income or being part of a technically-oriented industry would

affect respondents' attitudes toward cell phone use and identity theft. Because this was a qualitative study, it was not subject to the kind of quantitative analysis that might provide a definitive answer to the question of how membership in one group or another affected responses to interview questions. Nevertheless, based on the qualitative data analysis that was conducted, it does not appear that group membership influenced interviewees' responses.

Limitations

The primary limitation of this study was the sample size. Care was taken to select a representative biometrics company and typical cell phone users. However, a sample of 30 was not sufficient to permit generalization of the results to other informational technology employees or other private citizens who use cell phones.

The study was also limited geographically. For reasons of convenience and cost control, I only interviewed people who lived or worked in the Washington, DC, area. It was possible that this area was not representative of other parts of the United States.

The study was further limited by the wording of some interview questions. For example, I asked, "What can be done to reduce or eliminate identity theft?" It might have been more instructive to ask participants what steps *they* have taken rather than to solicit observations about the situation at large.

Conclusions

Based on the results of this qualitative study, several conclusions can be made. First, the cell phone is now considered an indispensable tool for both personal and business use. Data collection for this study involved finding people who used a cell phone regularly and who would agree to be interviewed. It would have been more

difficult to find individuals who did not own a cell phone than those who did. Also, although the sample consisted of people who were selected because of their business involvement (employees at a biometrics company) and those who were chosen simply because they own a cell phone, the latter were as likely as the former to distinguish between their personal and business use of cell phones.

Second, participants in this study, while agreeing that identity theft and loss of privacy have been exacerbated by the widespread use of cell phones, tended to see those threats as applying more to others than to themselves. This attitude is consistent with what has been discovered in other areas. For example, although there has been widespread criticism of public schools, the majority of parents are satisfied with their child's school (Tompson, Benz, & Agiesta, 2013). People see the social problems connected with cell phone use as being located "out there," and that well-intentioned individual behavior can offset any pernicious social trends.

Third, cell phone users are largely untouched by privacy concerns connected with using the phone to access social media. Most participants in the current study did use their phone for that purpose, and most of those did not see such use as a privacy risk. These results are consistent with findings by Butler et al. (2011), who studied the privacy awareness of Facebook users. Butler et al. administered a survey to 235 Facebook users and concluded that most were not knowledgeable about Facebook's changing privacy policies and default settings and were unaware of the potential consequences of their ignorance.

Finally, protecting cell phone users' privacy and identity is a shared responsibility of individuals, business, the cell phone industry, and government. People can help protect

themselves by engaging in responsible behavior: limiting where they use a cell phone and what kinds of personal information they divulge in phone conversations. Businesses can safeguard their information by instituting policies regarding cell phone use on the job. Cell phone manufacturers can enhance cell phone security by building into their phones protective measures such as voice or fingerprint recognition. Government can help by modifying its surveillance and data mining procedures in ways that safeguard national security while also preserving reasonable individual privacy.

Implications for Social Change

The timeliness of a study analyzing people's attitudes toward privacy has only been enhanced by events that have taken place since data collection for this study was completed. Concerns about the extent to which the National Security Agency has monitored and collected information about cell phone use have increased since revelations made by data Edward Snowden stole from the government and made public. Although attitudes toward privacy may be shifting, as I have suggested in this dissertation, recent events have made it clear that a significant percentage of the population—and their legislators—is concerned about how using a ubiquitous device on which people are increasingly dependent could compromise their privacy (Wintour, 2014).

This study can effect social change by informing the efforts of both government and private business to formulate policies that will protect individual privacy even as they promote national security. Cell phones have influenced individual behavior perhaps as much as any recent technological innovation. Their growing prominence has affected attitudes toward a range of issues, privacy being prominent among them.

Results of this study can also help in the ongoing fight against identity theft, a growing national and international problem. Identity theft predated the widespread use of cell phones, but cell phones have increased the avenues whereby identify thieves can operate. Identity theft was a $1.5 billion problem in 2011, according to the Federal Trade Commission ("Identity theft," 2012).

Recommendations

Based on the results of this study, several recommendations can be made. These are divided between recommendations for practice and recommendations for further research.

Recommendations for Practice

Recommendations for individual cell phone users were listed above: limit personal information stored on phones, do not divulge sensitive information over the phone, use security devices such as passwords and biometric-based identification, and enable cell phones with remote shutdown and data wiping capability. One of these suggestions also applies to cell phone manufacturers. For example, the recently released Apple iPhone 5S comes with built-in Touch ID fingerprint scanner. If such technology were standard equipment in the industry, rather than an add-on customers must purchase later, cell phone security would be improved.

Another recommendation made by some participants in this study is for greater government regulation of the cell phone industry. However, recent revelations about the extent of government monitoring of cell phone use has made many private citizens uneasy about whether their phone conversations are private. For these cell phone users, the prospect of greater government involvement in the industry might not be comforting.

Recommendations for Further Research

This qualitative study was an attempt to determine how cell phone use affects attitudes toward privacy and identity theft. Other qualitative studies could be designed to explore such attitudes among different groups. For example, I did not distinguish between users with smart phones and those with regular phones. It would be interesting to compare those two groups.

The vast majority of my participants were over the age of 30. It might be fruitful to compare that age group with a younger cohort. How do teenagers feel about cell phone security? How worried are they about identity theft?

I did not attempt to determine how much participants actually knew about cell phone technology. A qualitative study that included definitional questions could get at that kind of knowledge. For example, participants could be asked to proved definitions of terms such as phishing, encryption, and so forth.

Another promising direction is quantitative research. My sample was too small to determine how representative were participants' reports of such things as phishing, requests for personal information, losing a phone, or being a victim of identity theft. A quantitative study would enable a much larger sample and perhaps a greater ability to generalize the results.

Personal Reflections

This study was prompted by my own growing concern about the problem of identity theft. Although I have not been the victim of identity theft, I know people who have been. In particular, my work as a research and program management analyst with

the U.S. Army has made me aware of the implications of identity theft for members of the military.

I have also been interested to observe how the cell phone has evolved from novelty to status symbol to ubiquitous personal possession. Cell phones have changed people's lives, including my own. They affect how people obtain and use information, as well as how people conduct their personal and professional lives. The potential convergence of these two trends—increasing instances of identity theft and increasing use of cell phones—suggested itself as a worthwhile research topic. My research has confirmed my conviction that guarding privacy will continue to be a challenge. But it is a challenge, I am convinced, that is worth pursuing.

Summary

In this chapter, I discussed the results of a qualitative study of how cell phone use affects attitudes toward privacy and identity theft. Thirty people participated in individual, semistructured interviews. Although the sample was divided into three groups (employees of a biometrics company and individual users earning more than or less than $55,000 annually), it was not possible to draw meaningful distinctions among the groups based on their responses to interview questions. The cell phone is arguably the most consequential technological development of the last 25 years. It has changed people's behavior and relationships in myriad ways. As with any tool, a cell phone can be used for good and for ill. Minimizing its potential for harm is a responsibility shared by all: government, business, and private citizens. The results of this study will contribute to the responsible and productive use of cell phones and thus to the betterment of society.

References

Adams, C., & Dimitrinu, A. (2008). A two-phase authentication protocol using the cell phone as a token. *Journal of Information Privacy and Security, 4*(2), 23-39.

Akin, L. L. (2009). Activity monitors: AKA cell phone and computer eavesdroppers. *Forensic Examiner, 18*(2), 46-49.

Akopyan, D. A., & Yelyako, A. D. (2009). Cybercrimes in the information structure of society: A survey. *Scientific and Technical Information Processing, 36*(6). 338-350. doi:10.3103/S0147688209060057

Allen, A. (2001). Is privacy now possible? A brief history of an obsession. *Social Research, 68*(1), 301-306.

Alster, N. (2005). A touchy subject. *CFO, Color Photographics*, *21*(5). Retrieved from http://www.cfo.com/article.cfm/3739077/c_3759578?f=insidecfo

Anderson, H. (2011). iPad: The savior of digital publishing? *Journal of Internet Law*, *14*(10), 15-20.

Anderson, K. B. (2006). Who are the victims of identity theft? The effect of demographic. *American Marketing Association, 25*(2), 160-171. doi:10.1509/jppm.25.2.160

Angwin, J. (2010, July 30). The Web's new gold mine: Your secrets. *Wall Street Journal.* Retrieved from http://online.wsj.com/article/ SB10001424052748703940904575395073512989404.html

Argo, J. J., Dahl, D. W., & Machanda, R. V. (2005). The influence of a mere social presence in a retail context. *Journal of Consumer Research, 32,* 207-212.

Ashok, J., Shivashankar, V., & Mudiraj, P. S. (2010). An overview of biometrics. *International Journal on Computer Science and Engineering, 2*(7), 2402-2408.

Bednall, J. (2006). Epoche and bracketing within the phenomenological paradigm. *Issues in Educational Research, 16*(2), 123-138.

Berkowitz, S. (1997). Analyzing qualitative data. In J. Frechtling, L. Sharp, & R. Westat (Eds.), *User-friendly handbook for mixed-method evaluations* (pp. 14-21). Washington, DC: National Science Foundation.

Boulos, M., Wheeler, S., Tavares, C., & Jones, R. (2011). How smartphones are changing the face of mobile and participatory healthcare: An overview, with example from eCAALYX. *Biomedical Engineering Online, 10,* 24. doi:10.1186/1475-925X-10-24

Bourgeois, M. J., & Bowen, A. (2001). Self-organization of alcohol-related attitudes and beliefs in a campus housing complex: an initial investigation. *American Psychological Association, 20*(6), 434-437.

Bowers, C. A. (1988). *The cultural dimensions of educational computing: Understanding the non-neutrality of technology.* New York, NY: Teachers College Press.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340-347. doi:10.1177/1948550612455931

Brenner, J. F. (2010). Privacy and security: Why isn't cyberspace more secure? C*ommunications of the ACM*, *53*(11), 33-35. doi:10.1145/1839676.1839688

Bureau of Justice. (2011). *Identity theft.* Retrieved April 23, 2012, from http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=42

Butler, E., McCann, E., & Thomas, J. (2011). Privacy setting awareness of Facebook and its effect on user-posted content. *Human Communication, 14*(1), 39-55.

Charland, A., & Leroux, B. (2011). Mobile application development: Web vs. native. *Communications of the ACM*, *54*(5), 49-53. doi:10.1145/1941487.1941504

Clarke, N. L., & Furnell, S. M. (2007). Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security, 6*(1), 1-14. doi:10.1007/s10207-006-0006-6

Conti, J. (2008). The androids are coming. *Engineering and Technology, 3*(9), 72-75.

Costanzo, C. (2006). Suddenly, biometric ID doesn't seem like science fiction. *American Banker*, *171*(107). Retrieved from http://63.240.127.117/article.html?id=20060602HCMNR68G

Cowan, J. (2010). Why we'll never escape Facebook. *Canadian Business, 83*(10), 28-32.

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approaches.* Thousand Oaks, CA: Sage.

Creswell, J. W. (2005). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. Columbus, OH: Pearson Merrill Prentice Hall.

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Crompton, M. (2010). User-centric identity management: An oxymoron or the key to getting identity management right? *Information Polity: The International Journal of Government and Democracy in the Information Age*, *15*(4), 291-297.

Electronic Privacy Information Center. (2012). Electronic Communications Privacy Act. Retrieved February 27, 2012, from http://epic.org/privacy/ecpa/default.html

Federal Trade Commission. (March 2011). *Consumer SENTINEL network data book for January–December 2010.* Washington, DC: Author.

Gellman, R. (2009). Privacy in the clouds: Risks to privacy and confidentiality from cloud computing. *World Privacy Forum Report.* Retrieved from http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

Gershowitz, A. M. (2011). Password protected? Can a password save your cell phone from a search incident to arrest? *Iowa Law Review*, *96*(4), 1125-1175.

Ghencea, F., Voicu, A., Georgescu, M., Bratu, S., & Bisjan, A. (2011). The renewal of the public administration through the introduction of biometric technique in the peoples' record keeping activity: Psycho-social implications upon the individual. *Economics, Management and Financial Markets*, *6*(2), 429-437.

Giurgiu, L., & Barsan, G. (2008). The impact of the iPhone in education. *Bulletin Scientific, 13*(2), 57-59.

Glaser, B. G. (2004). Remodeling grounded theory. *Forum: Qualitative Social Research*, *5*(2). Retrieved from http://www.qualitativeresearch.net/index.php/fqs/article/viewArticle/607/1315

Goldsborough, R. (2010). Are you protecting your privacy online? *Teacher Librarian, 37*(5), 72.

Grimmelmann, J. (2010). Privacy as product safety, *Widener Law Journal, 19*(3), 793-827.

Harton, H. C., Green, L. R., Jackson, C., & Latané, B. (1998). Demonstrating dynamic social impact: Consolidation, clustering, correlation and (sometimes) the correct answer. *Teaching of Psychology, 25*(1), 31-35.

Hunt, K. (2004, Summer/Fall). The challenges of integrating data literacy into the curriculum in an undergraduate institution. *IASSIST Quarterly,* 12-15.

Identity theft cost Americans $1.52 Billion in 2011, FTC says. (2012, February 28). *The Huffington Post.* Retrieved January 13, 2014, from http://www.huffingtonpost.com/2012/02/28/identity-theft-cost-americans-152-billion-2011-ftc_n_1307485.html

Jain, A. K., Flynn, P., & Ross, A. A. (Eds.). (2008). *Handbook of biometrics.* New York, NY: Springer.

Joseph, A. E. (2006). *Cybercrime definition.* Computer Crime Research Center. Retrieved April 20, 2012, from http://www.crime-research.org/articles/joseph06/

Katzan, Jr., H. (2011). Ontology of trusted identity in cyberspace. *Journal of Service Science 4*(1), 1-11.

Kerr, O. S. (2009). Do we need a new Fourth Amendment? *Michigan Law Review, 107*(6), 561.

Kerr, P. (2009). Protecting patient information in an electronic age: A sacred trust. *Urologic Nursing, 29*(5), 315-318.

Kim, D. S., & Hong, K. S. (2008). Multimodal biometric authentication using teeth image and voice in mobile environments. *Consumer Electronics, IEEE Transaction, 54(*4), 1790-1797. doi:10.1109/TCE.2008.4711236

King, N., & Horricks, C. (2010). *Interviews in qualitative research.* Thousand Oaks, CA: Sage.

King, N. J., & Jessen, P. W. (2010). Profiling the mobile customer: Is industry self-regulation adequate to protect consumer privacy when behavioral advertisers target mobile phones? *Computer Law and Security, 26*(6), 595-612. doi:10.1016/j.clsr.2010.09.007

Ku, W., Chen, Y., & Zimmermann, R. (2009). Privacy protected spatial query processing for advanced location-based services. *Wireless Personal Communication, 51,* 215-220. doi:10.1109/ICDEW.2007.4400994

Lanois, P. (2010). Caught in the clouds: The Web 2.0, cloud computing, and privacy? *Northwestern Journal of Technology and Intellectual Property, 9*(2), 29-49.

Lanois, P. (2011). Privacy in the age of the cloud. *Journal of Internet Law, 15*(6), 3-17.

Lardner, R. (2010, February 17). Agency says parents need to know about kids' apps. *St. Paul Pioneer Press,* p. 3A.

Latané, B. (1981). The psychology of social impact. *American Psychologist, 36*(4), 343-356. doi:10.1037/0003-066X.36.4.343

Latané, B. (1996). Dynamic social impact: The creation of culture by communication. *Journal of Communication, 4,* 13-25.

Leedy, P. D., & Ormrod, J. E. (2010). *Practical research: Planning and design* (9th ed.). Upper Saddle River, NJ: Pearson Education.

Lenhart, A. (2009). More and more teens on cell phones. *Pew Research Center Publications*. Retrieved from http://pewresearch.org/pubs/1315/teens-use-of-cell-phones

Library of Congress. (2012). Bill summary and status, 2011-2012. S.1011. Retrieved from http://thomas.loc.gov/cgi-bin/bdquery/z?d112:s.1011

Longing, C. (2006). Your wireless future. *Business 2.0, 7*(4). Retrieved from http://money.cnn.com/2006/05/18/technology/business2_wirelessfuture_intro/

LoPucki, L. M. (2001). Human identification theory and the identity theft problem. *Texas Law Review, 80*(1), 89-134.

Mak, B., Nickerson, R. C., & Isaac, H. (2009). A model of attitudes towards the acceptance of mobile phone use in public places. *International Journal of Innovation and Technology Management, 6*(3), 305-326.

Maxwell, J. A. (2004). *Qualitative research design: An interactive approach* (2nd ed.). Thousand Oaks, CA: Sage.

Mayer-Schonberger, V. (2010). Beyond privacy, beyond rights: Toward a "systems" theory of information governance. *California Law Review, 98*(6), 1853-1885.

McNabb, D. E. (2002). *Research methods in public administration and nonprofit management: Quantitative and qualitative approaches*. New York, NY: E. Sharpe.

Mell, P., & Grance T. (2011). *The NIST definition of cloud computing.* National Institute of Standards and Technology. Special Publication 800-145. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Milne, G. R. (2003). How well do consumers protect themselves from identity theft? *Journal of Consumer Affairs, 37*(2), 388-402. doi:10.1111/j.1745-6606.2003.tb00459.x

Milne, G. R., Rohn, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs, 38*(2), 217-232. doi:10.1111/j.1745-6606.2004.tb00865.x

Merriam, S. B. (2009). *Qualitative research: A guide to design and implementation.* San Francisco, CA: Jossey-Bass.

Mobile Phones. (2010). In *Current Issues*. Retrieved January 13, 2012, from http://ic.galegroup.com.ezp.waldenulibrary.org/ic/ovic/ReferenceDetailsPage/ReferenceDetailsWindow?displayGroupName=Reference&disableHighlighting=true&action=2&catId=GALE%7C00000000LVZO&documentId=GALE%7CPC3021900112&userGroupName=minn4020&jsid=4aae315f0d77a38c0dd8ad

Morris, R. G. (2010). Identity thieves and levels of sophistication: Findings from a national probability sample of American newspaper articles 1995-2005. *Deviant Behavior*, *31*(2), 184-207. doi:10.1080/01639620902854969

Moustakas, C. (1994). *Phenomenological research methods.* Thousand Oaks, CA: Sage.

Nettle, D. (1999). Using social impact theory to simulate language change. *Lingua, 1008,* 95-117.

Nikolaev, A. G., Robbins, M. J., & Jacobson, S. H. (2010). Evaluating the impact of legislation prohibiting hand-held cell phone use while driving. *Transportation Research Part A: Policy and Practice, 44*(3), 182-193. doi:10.1016/j.tra.2010.01.006

Nowak, A., Szamrey, J., & Latané, B. (1990). From private attitude to public opinion: A dynamic theory of social impact. *Psychological Review, 97*(3), 362-376.

Nwatu, G. U. (2011). *Biometrics technology: Understanding dynamics influencing adoption for control of identification deception within Nigeria*. (Unpublished doctoral dissertation). Walden University, Minneapolis, MN.

O'Brien, J. A., & Marakas, G. M. (2011). *Computer software: Management information systems* (10th ed.). New York, NY: McGraw-Hill/Irwin.

Orwell, G. (1949). *1984.* New York, NY: New American Library.

PC Magazine (2912). *Definition of smart phone.* Retrieved April 20, 2012, from http://www.pcmag.com/encyclopedia_term/0,2542,t=Smartphone&i=51537,00.asp

Perlberg, H. (2012, February 18). Google faces privacy flap over iPhones, iPads. *St. Paul Pioneer Press,* p. 7A.

Pew Research Center. (2006). *The cell phone challenge to survey research: National polls not undermined by growing cell-only population.* Retrieved December 3, 2009, from http://people-press.org/report/276/

Pew Research Center. (2013). Cell phone ownership hits 91% of adults. Retrieved November 29, 2013, from http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/

Pheterson, I. (2011). Privacy—Between the devil and the deep blue cloud: Trends in biometric data collection and use. *Employee Relations Law Journal, 36*(5), 112-115.

Pocovinicu, A. (2009). Biometric security for cell phones. *Informatica Economica, 13*(1), 57-63.

Polkinghorne, D. E. (2005). Language and meaning: Data collection in qualitative research. *Journal of Counseling Psychology, 52*(2), 137-145.

QSR International. (2012). Introducing NVivo 9. Retrieved April 24, 2012, from http://www.qsrinternational.com/products_nvivo.aspx

Radha, N. N., & Karthikeyan, S. S. (2011). An evaluation of fingerprint security using noninvertible biohash. *International Journal of Network Security and Its Applications*, *3*(4), 118-128. doi:10.5121/ijnsa.2011.3411

Riley, C., Buckner, K., Johnson, G., & Benyon, D. (2009). Culture and biometrics: Regional differences in the perception of biometric authentication technologies. *Artificial Intelligence and Sociology*, *24*, 295-306. doi:10.1007/s00146-009-0218-1

Roberts, B. (2002). *Biographical research.* Philadelphia, PA: Open University Press.

Roberts, W., & Schreft, S. L. (2009). Data security, privacy, and identity theft: The economics behind the policy debates. *Economic Perspective, 33*(1), 22-30.

Robson, C. (2002). *Real world research* (2nd ed.). Malden, MA: Blackwell.

Ross, A., & Jain, A. K. (2004, September). *Multimodal biometrics: An overview.* Proceedings of the 12th European Signal Processing Conference, Vienna, Austria, 1221-1224.

Rubin, H. J., & Rubin, I. S. (2005). *Qualitative interviewing: The art of hearing data* (2nd ed.). Thousand Oaks, CA: Sage.

Shilton, K. (2009). Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection. *Communications of the ACM*, *52*(11), 48-53. doi:10.1145/1592761.1592778

Simbro, E. M. (2010). Disclosing stored communication data to fight crime: The U.S. and E.U. approaches to balancing competing privacy and security interests. *Cornell International Law Journal, 43*(3), 585-610.

Singleton, R. A., & Straits, B. C. (2010). *Approaches to social research* (5th ed.). New York, NY: Oxford University Press.

Sipior, J. C., Ward, B. T., & Mendoza, R. A. (2011). Online privacy concerns associated with cookies, flash cookies, and web beacons. *Journal of Internet Commerce, 10*, 1-16. doi:10.1080/15332861.2011.558454

Smith, A. (2011). *American and their cell phones.* Pew Research Center Report. Retrieved from http://pewinternet.org/Reports/2011/Cell-Phones.aspx

Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C. J. (2009). Flash cookies and privacy. *Social Science Research Network Working Paper.* Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862

Sonkamble, S., Thool, D., & Sonkamble, B. (2010). Survey of biometric recognition systems and their applications. J*ournal of Theoretical and Applied Information Technology, 11*(1/2), 45-51.

Stajano, F., & Wilson, P. (2009). Understanding scam victims: Seven principles for systems security. *University of Cambridge Technical Report No. 754.* Retrieved from http://www.cl.cam.ac.uk/techreports/

Statewatch. (2007). U.S. changes the privacy rules to exemption access to personal data. Retrieved January 6, 2012, from http://www.statewatch.org/news/2007/sep/04eu-usa-pnr-exemptions.htm

Stone, B., Flynn, E., Itoi, K., & Lee, B. J. (2004). Your next computer. *Newsweek*, *143*(23).

The Internet grows more dangerous. (2011). *Trends Magazine, 100,* 24-27.

Tian, L., Shi, J., & Yang, Z. (2009). Why does half the world's population have a mobile phone? An examination of consumers' attitudes toward mobile phones. *CyberPsychology and Behavior, 12*(5), 513-516. doi:10.1089/cpb.2008.0335

Tompson, T., Benz, J., & Agiesta, J. (2013). *Parents' attitudes on the quality of education in the United States.* Chicago, IL: Associated Press-NORC Center for Public Affairs Research.

Trochim, W. M. K., & Donnelly, J. P. (2006). *The research methods knowledge base* (3rd ed.). Mason, OH: Thomson Custom Publishing.

U.S. Department of Justice. (2003). The Privacy Act of 1974: 5 U.S.C. § 552a. Retrieved December 6, 2012, from http://www.justice.gov/oip/index.html

U.S. Department of Justice. (2011). Identity theft and identity fraud. Retrieved November 4, 2011, from http://www.justice.gov/criminal/fraud/websites/idtheft.html

Veer, E. V. (2010). *Facebook: The missing manual.* Sebastopol, CA: O'Reilly Media.

Weitzner, D. J. (2007). Beyond secrecy: New privacy protection strategies for open information spaces. *IEEE Computer Society, 11*(5), 96-105. doi:10.1109/MIC.2007.101

Wicker, S. B. (2011). Cellular telephony and the question of privacy. *Communications of the ACM*, *54*(7), 88-98. doi:10.1145/1965724.1965745

Wintour, P. (2014, January 8). Mass surveillance by security services should be reviewed. *The Guardian.* Retrieved January 13, 2014, from

http://www.theguardian.com/politics/2014/jan/08/surveillance-security-review-lib-dems-gchq-snowden

Wirtz, J., & Lwin, M. O. (2009). Regulatory focus theory, trust, and privacy concerns. *Journal of Service Research, 12*(2), 190-207. doi:10.1177/1094670509335772

Appendix A: Letter of Invitation

Dear _____

My name is Lewis Saunders and I am a doctoral candidate at Walden University. I am conducting a study as part of the requirements for my degree in Public Policy and Administration with a concentration in Information Management Systems. I would like to invite your organization to participate as a community partner.

I am studying attitudes toward privacy and identity theft and how these affect the behavior of cell phone users. The growing popularity of social media such as Facebook, Twitter, and Foursquare has led to suggestions that attitudes toward privacy are changing. GPS-equipped cell phones enable users' locations to be pinpointed with considerable accuracy, which has led to concerns about privacy. This study will lead to a better understanding of the potential misuse of cell phones and how that potential affects private industry, government, and private citizens.

If you decide to take part in the study, you will be asked to participate in a face-to-face or telephone interview. Interviews will be recorded and are expected to take less than an hour. Interview results will be confidential, and participants' names will not be used in any published results.

Thank you for your consideration. If you have questions about the study, please contact me. If you indicate that you will participate, I will provide additional information by e-mail or regular mail.

With kind regards,

Lewis Saunders

Appendix B: Informed Consent Form

Thank you for your interest in a study of how cell phone use is affected by privacy, security, and cybercrime. The purpose of this study is to explore how attitudes toward privacy and identity theft affect the behavior of cell phone users. With the growing popularity of social media, there is some evidence that attitudes toward privacy are changing. Cell phones provide a record of users' locations. The availability of such information to others has caused some concerns for its potential to lead to crimes such as robbery and kidnapping. This study will lead to a better understanding of the potential for misuse of cell phones and how that potential affects the attitudes of cell phone users.

The study will be based on individual interviews conducted by Lewis Saunders, a doctoral student at Walden University. Interviews will be conducted at a mutually convenient location. They are expected to last 60 minutes and will be audio recorded.

Lewis Saunders is an employee of the U.S. Army's Study Program in cooperation with the Army's Chief Information Officer/G6. That office is not initiating this research and has no oversight responsibilities regarding how it is conducted. As the researcher, Mr. Saunders will be a acting entirely in his capacity as a doctoral student; thus, there are no conflicts of interest in his role as primary researcher for this study.

You were selected to participate in this study because you are over 18 years of age and have knowledge and experience of cell phone use. Your participation in this research project is entirely voluntary. Participation will involve no known risks, and you will receive no rewards for participating. You are free to decline to answer any question posed, and you are free to withdraw from the study at any time without penalty.

Your responses to interview questions will be completely confidential. I will not use any identifying information in transcribing or reporting interviews. Your transcript will not include your name, gender, or residence or work location. Your interview responses will be coded with a number known only to me. I will keep all paper and electronic data in a locked file cabinet, with the key accessible only to me, for a period of 5 years, at which point all data will be discarded.

Be advised that I am legally bound to report to the proper authorities any illegal behavior that I become aware of as a result of conducting interviews for my research.

You will have an opportunity to review the transcript of your interview and check it for accuracy. Upon request, you will be provided with a summary of the study's results. You should keep a copy of this consent form.

You will not be compensated for participating in this study, and participation will provide no direct benefits to you. Society at large will benefit from this study's results, which are expected to inform ongoing legislative efforts to protect cell phone users.

If you have any questions about this research you may contact me. If you have questions about your rights as a participant, you may also contact Walden's Research Participant Advocate at 612-312-1210 or irb@waldenu.edu.

By signing below and returning the complete form or replying to this e-mail with the words “I consent,” I understand that I am agreeing to the terms described above.

Name (print name) _____ Date_____

Signature _____

Researcher (Lewis Saunders) _____ Date_____

Appendix C: Interview Questions

1. How does cell phone use affect individual and organizational privacy in your industry? In other industries?
2. To what extent is identity theft a problem in your industry? In other industries? Among the public at large?
3. How does cell phone use contribute to identity theft?
4. What could be done within your industry to make cell phone use more secure?
5. What other steps would reduce the incidence of identity theft?
6. What other thoughts do you have about data security in a digital age?
7. How often do you receive unsolicited text messages?
8. What social networking sites do you access from your cell phone?
9. How often do you receive requests for personal information from social networking sites or other websites?
10. How often have you been the target of phishing? Explain.
11. Do you blog?
12. Do you have your own website? Do you manage your own website?
13. Have you ever lost your cell phone? If so, do you think information was taken from it and used to target you for identity theft? How did or would you know? What are the implications/ramifications/possible results of identity theft?
14. Have you ever been the target of identity theft?
15. How did you learn about the theft?
16. Does using your cell phone in the way you do make you vulnerable to identity theft?
17. What can be done to reduce or eliminate identity theft?
18. Do you think that the biometrics industry has influenced (negatively or positively) your privacy and the protection against identity theft? Please provide examples.

Appendix D: Permission to Conduct Study

TO: Walden University
Institutional Review Board

FROM: Lewis O. Saunders
[illegible] W. Running Brook Rd
Columbia, MD [illegible]

Dear Mr. Saunders:

I give you permission to conduct data collection supporting the study titled: *The Relationship Between Cell Phone Use and Identity Theft*. *Data collection can be done by a mail or face to face with individuals within* [illegible], *Inc.*; however each individuals' participation will be voluntary and at his or her own discretion during lunch periods or after hours.

The researcher, Mr. Lewis Saunders, will ask individuals to participate in the study after providing him or her summarized description of the dissertation. Additionally, he will inform each of the potential participants that participation is strictly voluntary and a consent letter must be signed in order to participate. All data that will be collected will be encrypted using the researcher's personal computer. The results dissemination activities will take place only under the guidance and instructions from the Walden University IRB.

We understand that our organization's responsibilities include protection of participant's privacy by insuring the interviews will be conducted in secure locations. The security clearance possessed by Mr. Saunders will assure access to secured locations within the buildings used by [illegible]. At all times you will be using your personal resources; therefore, government resources are not required and all activities will be monitored by my Chief Operating Officer, Bob Landry. We reserve the right to withdraw from the study at any time if our circumstances change.

I confirm that I am authorized to approve research in this setting and understand that the data collected will remain entirely confidential and may not be provided to anyone outside of the research team without permission from the Walden University IRB.

Sincerely,

George Gallaghan
Chief Executive Officer / President
Phone: 703 [illegible]

[illegible]
[illegible]
[illegible]

Appendix E: Interview Themes

NODE LISTING OF CODING REPORTS (18 coding reports with 206 subcategories)
Titles sorted alphabetically

INTERVIEW QUESTIONS

1. Q01-Cell phone use affects privacy (2 subcategories)
   - a. Your industry (4 subcategories)
     - Blank - no answer - not applicable
     - Examples (13 subcategories)
       - *24-7 availability - eliminated privacy*
       - *Addiction*
       - *Email*
       - *Identity impersonation*
       - *Improved communications*
       - *Information compromise*
       - *Law enforcement*
       - *Restrictions on carrying create vulnerability*
       - *Secure info overheard*
       - *Secure info stolen*
       - *Solutions*
       - *Tracking personal info*
       - *Waive Fourth Amendment rights*
     - Little or no effect
     - Very much
   - b. Other industries (3 subcategories)
     - Blank - no answer - not sure - not applicable
     - Examples (16 subcategories)
       - *24-7 availability - eliminated privacy*
       - *Addiction*
       - *Email*
       - *Employee-boss relationship*
       - *Employees are targets*
       - *Government and any protected industry*
       - *Identity impersonation*
       - *Improved communications*
       - *Information compromise*
       - *Job security*
       - *Secure info overheard*
       - *Secure info stolen*
       - *Solutions*
       - *Tracking personal info*
       - *Travel industry*
       - *Waive Fourth Amendment rights*
     - Little or no effect

2. Q02-To what extent is identity theft a problem (3 subcategories)
   - a. Your industry (4 subcategories)
     - Huge problem
     - Non-existent or low
     - Not answered - not sure - not applicable
     - Same as other industry or public
   - b. Other industries (5 subcategories)
     - Huge problem
     - Moderate problem
     - Non-existent or low
     - Not answered - not sure - not applicable
     - Same as any industry or public
   - c. Public at large (5 subcategories)
     - Huge problem - on the rise
     - Not answered - not sure
     - Public responsibility
     - Public smaller firms
     - Same as any industry

3. Q03-How cell phone use contributes to identity theft (9 subcategories)
   - Apps - Cloud
   - Do not know
   - Easy to hack
   - False sense of security and trust
   - Lost stolen or misplaced cell phones
   - Sheer number of devices
   - Text transmissions email & messaging
   - Tracking
   - Unsecured and unencrypted personal info & contacts

4. Q04-How to make cell phone use more secure (6 subcategories)
   - Device security features
   - Not sure - NA
   - Nothing
   - Organizational policy
   - Remote access
   - User awareness and prevention

5. Q05-Other steps to reduce incidence of identity theft (3 subcategories)
   - Define identity theft
   - Not answered
   - Other steps to reduce identity theft (4 subcategories)
     - Device security features
     - Organizational policy
     - Remote access
     - User awareness & prevention

6. Q06-Other thoughts about data security in digital age (8 subcategories)
   - Device security features
   - Internet and websites
   - Not answered - none - not asked
   - Organizational policy
   - R & D
   - Technology advancement issues
   - Thievery is here to stay
   - User awareness & prevention

7. Q07-How often receive unsolicited text messages (3 subcategories)
   - How often (7 subcategories)
     - Always
     - Daily
     - Monthly
     - NA
     - Never
     - Seldom
     - Weekly
   - Seeking personal information
   - Unsolicited email spam

8. Q08-Social network sites access from cell phone (2 subcategories)
    - SN sites (11 subcategories)
        - Circles
        - Facebook
        - Google+
        - GroupMe
        - Instagram
        - LinkedIn
        - None or NA
        - Pinterest
        - Twitter
        - Vine
        - Word Games
    - Why accessed (9 subcategories)
        - Convenient from cell phone
        - Family and friends
        - Forum
        - Hobbies - Recipes – etc.
        - Inspiration
        - Networking
        - News & Business - World events
        - Professional connections
        - Word games

9. Q09-Personal info requests from SN & other websites (2 subcategories)
    - Answered both questions (2 subcategories)
        - Other websites (4 subcategories)
            - *Never*
            - *Not answered - NA - not asked*
            - *Often*
            - *Seldom*
        - SN sites (4 subcategories)
            - *Never*
            - *Not answered - NA - not asked*
            - *Often*
            - *Seldom*
    - One response to both questions (3 subcategories)
        - Never
        - Often
        - Seldom

10. Q10-How often target of phishing – explain (6 subcategories)
    - Examples
    - Frequency not given
    - Never
    - Not answered - Not sure - NA
    - Occasionally - seldom

- Often

11. Q11-Do you blog (3 subcategories)
    - NA
    - No
    - Yes

12. Q12-Website ownership management(4 subcategories)
    - Manage others
    - NA
    - Not own
    - Own and manage

13. Q13-Lost cell phone experience & results (4 subcategories)
    - a. Ever lost cell phone (5 subcategories)
      - No
      - Not answered
      - Yes - lost or stolen
      - Yes - misplaced temporarily
    - b. No - info was not used for IT
    - c. How did or would you know of IT (3 subcategories)
      - After loss or theft
      - Not answered - NA
      - Theoretical
    - d. Implications ramifications results of IT (7 subcategories)
      - Credit - Financial
      - Legal
      - None
      - Not answered - NA
      - Passed on to consumers
      - Personal passwords and information
      - Reputation - Security clearances

14. Q14-Have you been target of identity theft (3 subcategories)
    - No or unaware
    - Not answered - NA
    - Yes

15. Q15-How you learned about theft (6 subcategories)
    - Credit check - Security package
    - Friends
    - Media
    - Not answered - NA
    - Notified by vendor or financial institution
    - Professional training

16. Q16- Your cell usage vulnerability IT (3 subcategories)
    - No - why not
    - Not answered - NA
    - Yes – why

17. Q17-How to reduce or eliminate identity theft (21 subcategories)
    - Cannot be eliminated
    - Consumer education
    - Email protection
    - Fewer transactions using cell phones
    - Financial regulations - credit locks - credit reports
    - Government regulations
    - Identity verification
    - Isolate from society (tongue in cheek)
    - Manage personal data and passwords
    - More R & D
    - Not answered - NA - not sure
    - Opt out data mining websites
    - Safe surroundings and use
    - SafeGuard PII
    - Secure and encrypt personal information
    - Secured websites
    - Shred mail offers
    - Social network preventative measures
    - Software security
    - Stiffer penalties for perpetrators
    - Use cash

18. Q18-Biometrics influence and examples (3 subcategories)
    - Influence and given examples (3 subcategories)
      - Little or no influence
      - Negative influence
      - Positive influence
    - Not answered - NA – Unknown (3 subcategories)
      - Examples
      - Influence
      - Not asked
    - Would like to see

Curriculum Vitae

Lewis O. Saunders

Education

Present	Walden University, 155 5th Ave. S. Suite 200 Minneapolis, MN 55401
1994	Troy State University, Troy Alabama MPA Public Administration
1966	Adams State University of Colorado, Alamosa, CO BA Physics/Mathematics

Research Interests

Information technologies in the areas of data minding, biometric, cyber crimes, and cloud computing.

Dissertation

Mobile phone use has grown rapidly, from 97 million subscribers in 2000 to over 331 million at the beginning of 2012. With increased use of cell phones have come increasing concerns about privacy and identity theft. The purpose of this qualitative study was to determine how cell phone use is affected by attitudes toward privacy and identity theft. The study was based on social impact theory, according to which people's attitudes and behavior are affected by the strength and immediacy of others' attitudes and behavior. Research questions addressed the extent to which participants connect cell phone use with decreasing privacy and cybercrime, how the use of biometrics affects cell phone users' attitudes and behavior, and what steps should be taken to reduce the misuse of private information associated with cell phone use.

Teaching Interests

Information Management Technology, Emerging Technologies in Cloud Computing, Data Mining Techniques, Biometrics, and Cybercrimes

Career Positions

Physicist (1966-1967), U.S. Naval Weapons Laboratory, Dahlgren, VA
Physicist (1967-1968), National Bureau of standards, Washington, DC
Associated Engineer (1968-1971), RCA, Springfield, VA
Operations Research Analyst (1971-1976), Army Communications Electronics Office, Washington, DC
Computers Systems Command, Ft. Belvoir, VA
Operations Research Analyst (1976-1980), U.S. Army Concepts Analysis Agency (CAA), Bethesda, MD

Now at Ft. Belvoir, VA known as Concepts Army Agency (CAA)
Operations Research Analyst (1976-1980), U.S. Army (DAMO-C4, CIO/G-6, Washington, DC 20310-107
Operations Research Analyst (1980-1991), U.S. Army CIO/G-6, Rm C623, Pentagon and Ft. Belvoir, VA
Program Management Analyst (1991-Present), U.S. Army CIO/G-6, Rm C623, Pentagon, and Ft. Belvoir, VA

Accomplishments
Managing more than 133 studies and management support efforts and obtaining more than $32M in funds

Professional Activities
1966-present: Member of the America Society for Public Administration

Seminars/Conferences
Organized and sponsored for the last six years the Strategic Studies Conference at RAND Arroyo Center, Pentagon City, and Arlington, VA