ISSN No. 0976-5697

Volume 7, No. 7, Nov-Dec 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Communication Privacy Management and the Digital Footprint in Pervasive Computer-Mediated Communication

Prof. (Dr.) John Malala
Nicholson School of Communication
University of Central Florida
Orlando, Florida 32816

Abstract:The use of personal computers and smart phones as means of interpersonal communication has become standard and inescapable in the twenty first century. In many instances, it is expected that personal or group communication take place through the mediation of a personal computer or a handheld mobile device that is embedded with a microprocessor (such as a smartphone or a tablet computer). Pervasive computing is the growing trend towards embedding microprocessors in everyday objects so they can communicate information. The use of these devices to communicate over networks poses serious privacy concerns due to the fact that various service providers collect data about users in order to build digital footprints they use in order to present relevant advertising offers based on the person's identity. This study uses the Communication Privacy Management theory (CPM) in order to determine the degree to which people disclose private information in order to obtain some benefits in return. A survey of adults (18 and older) in the United States found that most people are unaware that they leave a digital footprint behind when they use various services, and that they do not utilize privacy techniques to protect their identity online.

Keywords: Digital footprint, communication privacy management theory, ubiquitous computing, pervasive computing, computer-mediated communication, internet privacy, cellphone privacy.

I. INTRODUCTION

The issue of privacy in the digital revolution has been a big concern for scholars since the turn of the century. As Shilton (2009) says, privacy is "the ability to understand, choose, and control what personal information you share, with whom, and for how long." With the proliferation of multifunction handheld electronic devices and smart phones, protecting one's privacy becomes a real challenge (see Such&Ravatsos, 2016). Shilton explains privacy challenges are related to smart phones in that not only do they place phone calls, they also surf the internet and serve as cameras, sound recorders and GPS devices. "Beyond chatting and texting, these features could make phone ubiquitous, familiar tools for quantifying personal patterns and habits," argues Shilton. While smartphones are portable computers that are easily accessible in times of necessity, their pervasive nature also means that it is nearly impossible for users to conceal their identities, habits, and whereabouts. Privacy is a fundamental right that is bestowed on all people. This fundamental right, and the sensitivities associated with its infringement when the content of a smart phone is accessed by an unauthorized party, was upheld by the United States Supreme Court in 2014. The Court recognizes that smart phones that are connected to networks use software applications that keep sensitive private information about their owners. In fact, in the case of*Riley v. California* (2004) the Court ruled that a person's privacy is so important that, even in the case of an arrest, police officers must obtain a search warrant in order to access the contents of an arrestee's device. The Supreme Court argued that:

> There is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cellphone, with all that it contains, who is the exception.

According to the Privacy Rights Clearinghouse (2014), a mobile phone can reveal many things about a person as "it's safe to assume that anything you do on your smartphone and any information you store is at risk of being snooped on if you don't take proper precautions." Individuals' right to privacy is so important that peoplewant to have a great deal of control over data that uniquely identify them, their health, and their lifestyle. In a networked world where services, devices, and appliances interact seamlessly, maintaining total influence over personal information can be very challenging. Hence, argues the Court in Riley v California, "most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so," says the Court. "When privacy-related concerns are weighty enough a search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee."When talking about the concerns of cell phone privacy, Arvidson (2014) argued that:

> Safeguarding mobile phone users' data has become a central issue for privacy rights advocates, who say that mobile phone data is highly insecure and cellphone users have become easy targets for surveillance because of the global positioning system tracking capabilities of many of today's phones.

The use of personal computers and smart phones as means of interpersonal and mass communication has become standard and inescapable in the twenty first century. In many instances it is expected that personal or group communication takes place through the mediation of a personal computeror a handheld mobile device that is embedded with a microprocessor such as a mobile phone or a tablet computer. All over the world, people of all ages exchange information, send and receive messages, download and upload files to the internet, and share all their activities and movements with the world on social media from their smart phones, tablets, and personal computers virtually every second. Banks, airlines, schools, hotels, government organizations, and perhaps all industries have now made it possible for people to use mobile phones to conduct normal business. Conversations and transactions take place every day between various devices and platforms in an interoperable manner. The fact that business is conducted on personal smart phones carries a risk of personal data being shared inadvertently with people who should not have access to the information. Information technology experts argue that communications technologies have advanced so much that their applications and impacts raise serious concerns about privacy; and that the need for more research that explores these concerns is paramount (see Osatuyi, 2014; Xu and Belanger, 2014).

A. PERVASIVE COMPUTING

According to the Internet of Things, “pervasive computing (also called ubiquitous computing) is the growing trend towards embedding microprocessors in everyday objects so they can communicate information.” Experts use the terms pervasive and ubiquitous interchangeably. Devices are constantly available and completely connected in a pervasive computing world. Similarly, Webopedia defines pervasive computing as “the idea that almost any device, from clothing to tools to appliances to cars to homes to the human body to your coffee mug, can be imbedded with chips to connect the device to an infinite network of other devices.” Pervasive computing refers to the modern technological culture that takes computing beyond personal computers. As Webopedia indicates, pervasive computing combines “network technologies with wireless computing, voice recognition, Internet capability and artificial intelligence … to create an environment where the connectivity of devices is embedded in such a way that the connectivity is unobtrusive and always available.”Satyanarayanan (2001) states that the essence of the vision behind pervasive computing is "the creation of environments saturated with computing and communication capability, yet gracefully integrated with human users.”

Pervasive computer-mediated communication comes with many privacy and security risks that are not sometimes known by consumers. In fact, Youn, Kim and Lim (2014) stated that “along with the rapid information communication systems, the privacy of entities is more important now than ever before.” They recognized that the pervasive nature of computer-mediated communication and the privacy issues that ensue are due to the mobility of underlying devices such as smartphone, tablet, and mobile gadgets.The literature suggests that there is a special academic interest in trying to understand the dynamics of privacy as it relates to the networked world. Specifically, scholars are interested in knowing who has access to the data that they voluntarily provide in order to use services online (Bélanger&Crossler, 2011; Diney& Hart, 2006; Stewart &Segars, 2002)

B. TIMELINESS AND RELEVANCE OF THE PAPER

On September 22, 2016, Yahoo publicly confirmed a massive data breach of its services following an investigation of claims made by a hacker earlier that summer that they had access to 200 million user accounts, and that they were selling these data online on dark market websites. Hackers who called themselves “Peace” claimed to have data that included Yahoo usernames, passwords and dates of birth. Yahoo’s confirmation of the breach was repeated on various media outlets informing viewers, listeners, and readers that information from at least 500 million Yahoo accounts was stolen from the company in 2014 by what the company believed to be a state-sponsored actor.

The data breach worried giant U.S. telecommunications companies such as AT&T and Verizon because of their partnerships with Yahoo, and how this incident may have put their customers at risk. Fuscaldo (2016) explained that fifteen years earlier, “AT&T and Yahoo inked a partnership when AT&T was operating under the name SBC Communications bringing Yahoo’s search engine, email and other services to AT&T’s broadband customers.” At the time of the breach the ad revenue-sharing deal between the two companies was still in effect. Thus, whether AT&T's customers knew it or not, they were by default getting access to Yahoo’s services including email, which also means that they may have been put to risk due to the data breach at the giant internet company. The fact that Yahoo was not aware of the massive data breach until two years after it occurred is a point of concern for everyone who communicates or exchanges information via computer networks on mobile devices, laptops, and desktop computers. As Perlroth (2016) stated, “how the company discovered the hack nearly two years after the fact offered a glimpse at the complicated and mysterious world of the underground web.” There were many other web and telecommunications services that had direct profit-sharing relationships with Yahoo or owned completely by the internet giant.

Griffin (2016) explained that hundreds of millions of people whose services depend on Yahoo might not even know that they may be affected by the data breach. With one billion monthly users, Yahoo is one of the internet’s busiest sites and its free email service is one of the oldest with which many users have built their digital identities. Services offered by Yahoo allow users to verify and prove that they are who they claim to be in order to access bank accounts, medical information, photo albums, etc.

II. THEORETICAL FRAMEWORK

The present study is founded in the Communication Privacy Management Theory (CPM), initially known as the Communication Boundary Management (Petronio, 1991). This theory is an evidence-based systemic theory that describes the decision-making process that leads people to reveal or conceal information they consider private. According to the CPM theory, individuals control and set some limits or boundaries around what they are willing to share with various partners. The boundaries are metaphors used by Petronio to draw the line between public information and private information. The sharing of private information depends on the perceived returns and costs of what they are willing to disclose about themselves.

Private information is only shared with people who are seen as partners (e.g. friends, family, co-workers, service providers, etc.) Therefore, CPM theory is a management method that describes the rules people use when considering sharing private information by controllingthe levels of accessibility. In other words the person sharing the private information has control over (sets the boundaries between) who has and who must not have access to information about themselves. Thus, a person's decision to disclose or not disclose private information depends on the boundaries set by the individual. These privacy rules must be negotiated by the parties, and the person who shares private information expects this information to be used within the framework of these negotiations. Even though the emphasis of CPM studies has been on relationships because of disclosure (McBride & Bergen, 2008), the theory has been applied in various contexts, including family communication, social media, health communication, personal relationships, and work environments (Miller &Weckert, 2000; Petronio, 2013; Kanter& Robbins, 2012; Vik and Bates, 2016; Osatuyi, 2014; Ngcongo, 2016; Such &Rovatsos).

A. PRIVACY CONCERNS IN PERVASIVE COMPUTING

The latest Yahoo data breach incident leads to not only a security concern but also to real privacy worries. As the use of smart phones and embedded devices continues to grow exponentially, it becomes possible for many users not to be aware of the fact that they are actually connected to the internet when they use their phones. People who read their email on their smart phones, and those who download free apps leave a trove of digital footprints that serve as a form of payment to advertisers for free services that they use online in the form of personal digital currency. The lack of transparency in third-party tracking applications is a serious cause for concern because it is unclear how the data are stored and used. Tracking people's activities online is part of a shockingly large ecosystem of data collection used by websites, search engines, advertisers, and many other organizations. Companies are able to build detailed profiles of internet users based on a combination of personally identifiable information that people submit when they download apps or when they fill out forms online. Anonymized data obtained through people's online searches are part of this large ecosystem.

B. THE DIGITAL FOOTPRINT

Hewson (2013) defines digital footprint as "a person's online activities, including their use of social networking platforms." The notion of digital footprint can be explained in that every time people online whether knowingly (e.g. visiting a website, searching for something through a search engine, voluntarily filling out a form online, reading email on Yahoo mail or any other service) or unknowingly such as using one's smart phone to send text messages via a default application or third-party app such as WhatsApp or Viber, or whenever they use social media sites regardless of the device used, they leave behind traces of their activities. These traces of online activities are called digital footprints. Telecommunications companies, including free online service providers utilize tracking software and systems that allow them to retrace users' "digital footsteps." Unlike physical footprints, people's digital footprints reveal more about them than they realize. The information that users leave behind allow trackers such as the maker of the internet browser or the company that provides the free service to know everything from people's preferences to their identities and to aggressively personalize their services to users. In fact, Zhang (2016) argues that internet "users want to limit the sharing and usage of their information to what is necessary to achieve their goals (and preserve their overall privacy)," but that it is on the other free service providers have something else in mind: they seek to "collect and utilize user information for use in targeted promotions and advertisements, which is one of their primary sources of revenue."

There's an assumption that people know what they are getting into when they use smart phones, download apps, or sign up for social media. While there's no reason to argue that in many cases people do weigh in their decision before disclosing personal information, Kehr et al (2015) criticizes existing research on information privacy because it "has mostly relied on the privacy calculus model, which views privacy-related decision-making as a rational process where individuals weigh the anticipated risks of disclosing personal data against the potential benefits."The fact of the matter is that many people are ignorant of privacy issues in pervasive computing. Unbeknownst to users these free services are not exactly free. Instead of paying with dollars and cents, users of free services pay to companies that offer these services with their digital footprints and digital identities (Angwin, 2016). For most people free digital services have become the norm in the 21st century that they have no idea of the risk associated with obtaining something they do not pay for. In other words, people expect digital content and digital services to be free. From email services (e.g. Yahoo mail, Google Gmail, Microsoft's Hotmail etc.) to social media accounts (e.g. Facebook, Twitter, Instagram, YouTube, etc.) to Voice-over-IP services (Skype, Viber, WhatsApp, etc.), to shareware and freeware apps, users around the world demand free stuffs for use on their smart phones, tablets, and personal computers. As already indicated above, while the websites that people use, apps they download, and services they use are free, these organizations collect data about users in order to better personalize their experiences, and present relevant advertising offers based on the person's identity.

C. THE POTENTIAL FOR HARM

Collecting people's data in order to build profiles for advertisement purposes may cause serious harm to users. For example, Libert, Grande, and Asch (2015) showed that unauthorized online access of a patient's digital footprint can be harmful when websites use tracking techniques to connect people who are seeking health information online with third parties such as online advertisers. They argued that "records of visits to pages for sleep apnea, depression, or addiction treatment can be resold to organizations that want to know who is interested in these topics." Such unauthorized disclosures can be harmful to unsuspecting internet surfers because of the fact that digital footprint trackers use techniques that make it difficult for an internet user to conceal their online activities. Unlike cookies that can be deleted after each use, trackers use a technique browser fingerprint, which is a new method of tracking that uses computer specs and characteristics to, not only identify the person, but also to correlate one's searches and surfing across the internet.

Tracking a person's digital footprint could interfere with the individual's life offline. Access to one's full profile through complex data mining from mobile communications, social networks, search engines, as well as across various apps in a connected world can contribute to unfair business treatment such as price discrimination and decreased creditworthiness. The problem with tracking, as Shilton (2009) pointed out, is that "location traces can document and quantify habits, routines, and personal associations." This can be dangerous because a person's location might reveal their babysitter's home, their child's school, their shopping itinerary, the time they go to work to the time they return home, their regular trips to a therapist or doctor, the times when they are out of town etc. "These traces are easy to mine and difficult or impossible to retract once shared," Shilton says. While this study is not concerned with quantifying instances of such misuses, it does elucidate what is possibly happening behind the scenes and completely out of consumers' control. In the United States where insurance companies are prone to deny coverage to people whose profiles suggest some risks, the digital footprint can be misused by imposing a more expensive insurance coverage on someone or producing disparaging health reports about a person.

Based on the communication management theory, it is necessary to try to find whether smart phone users deliberately share private information without setting boundaries, or whether this disclosure is done without their knowledge for lack of propereducation. Consumer Reports (2016) argued that "companies should tell you in simple language about the kinds of personal information they collect and how your information could be shared, sold, and used. You should be given clear options to control the collection and use of your data." Shiltonarticulates that "privacy decisions have many components, including identity (who is asking for the data?), granularity (how much does the data reveal about me?), and time (how long will the data be retained?)" People should only share in order to gratify their needs (see Quinn, 2016).

Xu and Belanger (2013) stated that "the extensive display of personal information by users of social media requires greater stress on theoretical, epistemological and empirical research in information privacy." They argue that "privacy is an ever-present and mounting concern among multiple stakeholders including business leaders, privacy activists, scholars, government regulators and consumers." Li and Slee (2014) argue that "the most notable factors that influence willingness to provide personal information online are information privacy concerns...in e-commerce and health care settings." These concerns revolve around the question of "how the information is used."

Nonetheless, the body of literature available on issues of privacy in pervasive computer-mediated communicationshows that most of what has been discussed remains theoretical, argumentative, or positional. None of the previous studies has investigated people's attitudes toward sharing private information with various organizations, or the degree to which individuals are worried about who might have access to their private information online, and how this information could be used. This study offers the first glimpse of knowledge on the dynamics surrounding the use of ubiquitous computing and the management of communication privacy. Therefore, in order to try to understand people's mindset on internet privacy, boundaries, and rules between parties, the following research questions have to be answered:

RQ1: To what extent do adults set boundaries for their personal digital footprint between sensitive and non-sensitive information?

RQ2: To what extent do adults willingly offer to share private information in order to enjoy the benefits of the digital lifestyle?

RQ3: What factors are taken into consideration for free services in exchange to personal identifying information?

RQ4: To what extent does the adult population equally agrees on the reasonable length of time various agencies or organizations should be allowed to keep users records?

RQ5: What percentage of adults is aware of and uses techniques and tools available to protect their digital footprint?

III. METHOD

As indicated in the first chapter of this paper, this research sought to addressthe issue of the extent to which users of networked devices agree to share private information in order to gratify their needs in the context of the Communication Privacy Management Theory. There is more than one set of data that was used for this paper. Data for this study come from four sets of surveys conducted by the PEW Research Center (PRC) for a period of a little over one year, starting from January 27, 2014 ending on February 16, 2015 as part of what was called the "Internet Project."The data were obtained by permission from PRC.

Participants to these surveys were adults ages 18 and older. The initial panel was told that they will receive 4 online surveys about current issues, some of which relate to technology. They were also told that the surveys will occur over the course of a year (once every 3 months). Subjects were also told that in addition to the online surveys, approximately once a month the PRC would invite 10-12 individuals from this special group to participate in a 45-60 minute online focus group chat. Members of the focus groups were paid a $35 reward per each session.

Most of the focus groups sessions dealt with technology and various privacy issues in what was labeled "Privacy Panel #1, Privacy Panel #2, Privacy Panel #3, and Privacy Panel #4)." The number of participants per panel where consecutively N1=607; N2=498; N3=475 and N4=461. Details of measures used are found in Tables 1 through 7 in the results section below. For example, in one of the panels participants were presented certain areas of modern life and communications platforms (content of email, content of text messages, content of telephone conversation, among others), and were asked to indicate whether they thought these conversations and content of data in these areas were sensitive or not (see Table 1). The measure were on a four-point Likert scale from "very sensitive" to "not all." For the purpose of this research, a Chi-Square test was performed to determine whether the subjects viewed contents of each of the measures as equally important.

Another Likert scale (Strongly Agree to Strongly Disagree) set of questions selected from that data measure that was tested was the degree of confidence that participants had on maintaining anonymity and ensuring that their records contain accurate information (see Table 2). As for the previous set, another Chi-square test was used to determine the extent to which participants' responses were in agreement among all three measures. Overall, as shown in the findings section below, several Likert scale measures were used, and Chi-Square tests were performed in order to determine whether adults' attitudes and privacy-related practices were evenly distributed in the populations. The choice of the Chi-Square test was appropriate because the approach of the study was to look at frequency distributions rather than any type of correlation between variables.

IV. FINDINGS

The Communication Privacy Management theory deals primarily with identifying which information are private (sensitive) and which one is not. The first research question sought to determine to what extent adults set boundaries of their personal digital footprint between sensitive and non-sensitive information. A chi-square test of goodness-of-fit was performed to determine whether information about related to the ten aspects of privacy were equally seen as being very sensitive areas to consumers. The result of the test (see Table 1) shows that the population did not consider information in all ten aspects as equally very sensitive, X^2 (27, N = 607) =149.648, *p*< .00. As seen on Table 1, the result of the survey shows that 9 out of 10 adults consider their Social Security Number as a very sensitive piece of information. Nearly half of the population thinks the same about the content of their phone conversations, email, text messages, and the state of their health. Less than half consider phone numbers they have called or texted as being very sensitive information. Finally, only 1 in 4 people consider websites they visit and searches they make online using search engines to be very sensitive information.

Table 1

% of Adults who reports varying levels of sensitivity about the following information

ASPECTS	*Very Sensitive*	*Somewhat Sensitive*	*Not too Sensitive*	*Not at all*
Your Social Security number	90	5	2	1
Content of your phone conversations	54	27	13	4
Content of your email messages	52	25	13	7
Content of your text messages	49	26	13	8
Details of physical location over a period of time, gathered from the GPS data from your cell phone	50	32	11	5
Numbers you have called or texted	45	30	16	6
Your friends and what they are like	22	46	23	7
Websites you have visited	27	43	20	8
Searches you have made using search engines	24	41	22	10
State of your health and medication you take	55	26	12	5

X^2 (27, N = 607) =149.648, p< .00.
Yates' Chi-square=138.365; p< .00. Refused responses are not shown

CPM theory argues that individuals disclose private information in exchange to some perceived benefits. Therefore, the second research question sought to determine to what extent adults willingly offer to share private information in order to enjoy the benefits of the digital lifestyle. A chi-square test of goodness-of-fit was performed to determine whether there was an equal agreement (easiness to by anonymous online, willingness to share information with company in exchange for free services, and difficulty to remove inaccurate information about oneself online) or a disagreement on the three measures of perceived level of difficulty to take action. The result of the test (see Table 2) shows that the population did not equally agree on the level of easiness to be anonymous online, the willingness to share information with companies in return for free services, and the level of difficulty to take action in order to correct inaccurate information about oneself, X^2 (6, N=607) =116.343,*p*< .00. As seen in Table 2, in total 8 out of 10 adults think it not is easy to remain anonymous online. The survey also shows more than half of the adult population said they either agree or strongly agree that they are willing to share some information about themselves with companies in order to use online services for free. Meanwhile 9 out of 10 people agree or strongly agree that it would be very difficult to remove inaccurate information about oneself online.

Table 2

% of Users' Attitude towards Privacy and Usability

	Strongly Agree	*Agree*	*Disagree*	*Strongly Disagree*
It is easy for me to be anonymous when I am online	3	20	52	24
I am willing to share some information about myself with companies in order to use online services for free	4	51	31	13
If inaccurate information about me got posted online, it would be very difficult to get it removed	39	49	9	3

X^2 (6, N=607) =116.343, p< .00
Yates' Chi-square=109.4, p< .00. Refused responses are not shown.

In order to determine how adults make disclosure decision, the third research question sought to determine how people make a decision to download free apps in exchange to personal identifying information. This was very important because it also adds some clarity to the CPM theory in which suggests that people weigh in their decisions before making a disclosure. As seen in Table 3 below, the population did not equally agree on factors that influence their download decisions, X^2(9, N=242)= 78.357, *p*< .00.In fact, 5 in 10 people said it is very important that the app has positive ratings and reviews from other users. Meanwhile 6 out of 10 people also reported that the fact that the app provides clear information about how it will access or use your data is a very important factor that influences their download decision. Knowing someone who has used the app or downloading an app that has already been downloaded a certain number of times were not very important factors to the majority of the population.

CPM is a rule-based theory that requires partners to negotiate the boundaries of the disclosure. In the context of various service providers, it is crucial for users to agree to how long organizations are allowed to retain personal information or records after the service has been rendered. The fourth research question sought to determine whether the population equally agrees on the reasonable length of time that various agencies or organizations should be allowed to keep users records.

Table 3

% of Adults expressing importance on factors influencing their decision to download an App.

	Very important	*Somewhat important*	*Not very important*	*Not at all important*
The app has positive ratings and reviews from other users	51	37	8	4
The app has been downloaded a certain number of times	22	36	28	14
The app provides clear information about how it will access or use your data	59	31	9	1
Someone you know has used the app	17	38	26	18

X^2(9, N=242)= 78.357, p< .00.
Yates' Chi-Square = 69.396, p<.00

The results of the survey designed to answer this research question are on Table 4 below. The result of a chi-square goodness-of-fit shows that the population is not equally in agreement with which organization should keep one's record for any given length of time or whether any organization should keep them at all, X^2(30, N=498)= 145.286, *p*< .00. The majority of adults agree that it is reasonable for cellular phone companies, government organizations, and credit card companies to retain users/customers' records or archives of their activities between a few weeks to as long as they need to. Meanwhile the adult population is divided between those who believe search engines and social media websites should keep users' records/archives of their activities and those who say that search engines should not keep these records at all.

Table 4

Reasonable length of time for the following companies or organizations to retain users/customers records or archives of their activity

Organization	*A few weeks*	*A few months*	*A few years*	*As long as they need to*	*They shouldn't save any information*	*Doesn't apply to me*
Your cellular telephone company	11	21	14	16	24	10
Your search engine provider	19	12	6	8	40	12
Your e-mail provider	12	19	11	15	32	8
The social media sites you use	14	11	5	4	40	22
Government agencies	8	8	23	28	22	8
Your credit card companies	6	14	28	22	13	13
The online advertisers who place ads on the websites you visit	18	7	1	5	50	14

X^2(30, N=498) = 145.286, p< .00
Yates' chi-Square = 129.661, p < .00

In order to test the CPM theory on the actual application of setting boundaries between private and public information in pervasive computer-mediated communication, the fifth research question sought to determine what percentage of adults were aware of, and used techniques and tools available to protect their digital footprint. The results for this question are found in Tables 5 and 6 below. As seen in Table 5, the study found that except for 6 out of 10 adults who refused to provide information that was irrelevant to a transaction or cleared the browser for cookies, most of the boundary-setting privacy techniques available to them were not used. For example, only 1 in 10 added a privacy-enhancing browser plugin like Do Not Track Me or Privacy Badger to their online surfing experience. Similarly 1 in 10 adults used a service that allows you to browse the Web anonymously, such as a proxy server, Tor software, or a virtual personal network (VPN), and also 1 in 10 adults browsed the internet anonymously on a public computer.

Table 5

% of Adults who have ever used techniques or tools to protect their privacy online

	Yes	*No*	*Does not apply to me*	*Don't know*
Used a temporary username or email address	25	56	9	5
Added a privacy-enhancing browser plugin like Do Not Track Me or Privacy Badger	9	72	8	8
Given inaccurate or misleading information about yourself	24	60	7	6
Set your browser to disable or turn off cookies	34	43	8	12
Cleared cookies and browser history	59	22	7	8
Used a service that allows you to browse the Web anonymously, such as a proxy server, Tor software, or a virtual personal network (VPN)	9	67	9	10
Encrypted your phone calls, text messages or email	10	68	10	10

Decided not to use a website because they asked for your real name	23	55	12	7
Deleted or edited something you posted in the past	29	46	14	8
Asked someone to remove something that was posted about you online	11	63	15	7
Used a public computer to browse anonymously	12	68	12	6
Used a search engine that doesn't keep track of your search history	15	52	11	19
Refused to provide information about yourself that wasn't relevant to the transaction	57	23	9	8

N=498

Table 6

% of Adults who adopted the following tools or strategies to make their communications and activities private since learning about U.S. phone and internet monitoring.

	I have adopted this	*I have not adopted this, but have considered it*	*I have not adopted this and have not considered it*	*I don't know what this is*	*Not applicabl e to me*	*Refused*
Used a search engine that doesn't keep track of your search history	10	12	53	13	12	1
Adopted email encryption, such as PGP	2	10	46	31	11	1
Adopted mobile encryption for calls or text messages	4	8	48	24	15	2
Used more complex passwords	25	12	48	6	8	1
Proxy servers	3	7	41	33	13	2
Added a privacy-enhancing browser plugin like DoNotTrackMe or Privacy Badger	5	7	43	31	13	1
Changed your privacy settings on social media such as Facebook or Twitter	19	6	44	4	26	1
Used locally-networked communications such as FireChat	1	4	42	37	14	1
Used anonymity software such as Tor	2	5	40	39	13	1
Used another software or network tool to make your activities more private	3	9	60	14	12	1

X^2(36, N=417) = 177.36, p< .00.
Yates chi-square =159.259, p< .00. Refused responses shown but not included in the calculation.

When some of the variables in the question above have been removed and other added, users are given more choices to see whether they have considered using any of the privacy techniques despite the fact that they may not have done so yet (See Table 6). The result of a chi-square goodness-of-fit shows that the population is not equally in agreement with whether they have adopted the privacy technique, or whether they have not adopted the privacy techniques but have considered it, and whether they have not adopted the techniques and have not considered it; or whether they don't even know anything about the technique, X^2 (36, N=417) = 177.36, *p*< .00. The majority of the population has not considered using an online privacy technique.

Finally, CPM theory assumes individuals want to be in control of their private information, and that they want to decide with whom to make the disclosure, when, under what condition and for how long. The results of the test of variables in which people expressed the importance of having control in a number of privacy practices are shown on Table 7 below. While the Chi-Square test shows that the degree of importance was not equally distributed among all 10 measures, more than 7 out of 10 people said it is very important to be in control of who can get information about them; and almost the same proportion said the same about being able to share confidential information with someone they trust, not having someone watch them or listen to them without their permission, and controlling what information is collected about them.

Table 7

% of Adults expressing the importance of having control over certain privacy practices:

	Very important	*Somewhat important*	*Not very important*	*Not at all important*	*Don't know / doesn't apply*
Being in control of who can get information about you	74	19	3	1	1
Not having someone watch you or listen to you without your permission	67	20	8	1	-
Controlling what information is collected about you	65	25	5	1	1
Having individuals in social and work situations not ask you things that are highly personal	44	36	13	2	4
Being able to have times when you are completely alone, away from anyone else	55	30	9	2	2
Being able to share confidential matters with someone you trust	72	21	2	1	1
Not being monitored at work	28	28	22	6	15
Not being disturbed at home	56	29	9	2	2
Being able to go around in public without always being identified	34	29	25	6	4

X^2 (32, N=461) = 161.322, p< .00.
Yates' Chi-Square=140.879 Yates' p < .00.

**Note: Use of chi-square test was not appropriate because expected frequencies of less than 5 was in more than 20% of the cells. Therefore Yates' corrections were applied.*

V. DISCUSSIONS AND CONCLUSION

This study was the first major attempt to try to quantify understanding of the interplay between people's actions in pervasive computer-mediated communication and their level of awareness as to how their digital footprint could have an impact on their desire to protect their privacy online by using the Communication Privacy Management theory. The need or desire by the adult population to be in control of their privacy was clearly observed and documented. Overall the study found that the majority of the adult population (7 out of 10) wants to be in control of their private information. The same proportion of the population also does not want someone else watching or listening to them without their permission. These adults indicated also that it is very important for them to be in control of what information if collected about them as well as be able to only share sensitive information with someone they trust.

However, the majority of the same people who want to have total control over their private information, and who do not want unauthorized individuals to listen to their conversation or collect information about them, are not using tools and techniques that are available to them in order to maintain their privacy online. Not only are they not using privacy-enhanced tools and techniques, they have not considered using these tools/techniques or they don't know that these tools exist. For example, only 1 in 20 people added a privacy enhancing browser plugin to remain anonymous online. The discrepancy between what people want and what they are not doing could clearly be a matter of ignorance. The study found that 9 out of 10 people consider their Social Security number as a very sensitive piece of information while the overwhelming areas of their lives that can allow advertisers and hackers to build a complete profile of them were not considered very important. The adult population does not seem to realize that their digital footprint that includes things such as their medical records, search engine queries, online activities, friends, and various associating aspects of their lives can be as harmful as someone stealing their social security number.

There an assumption that most adults in the U.S. have learned over the years that their social security number is their identity but not much is known by society that in today's digital landscape a person's identity is built around associating many of the person's activities online. There's a need for sustained coordinated education on the issue of privacy in the digital landscape and how to protect it. Benchmarks must be set to monitor progress in people's understanding of their digital footprint and the actions they take to protect themselves in the use of their smart phones and personal computers online. Finally, there's a need of long-term longitudinal or time-series studies that will include treatment at various stages in order to influence people's behavior regarding privacy in the digital environment.

VI. REFERENCES

[1] Angwin, J. (2016). Protecting Your Digital Privacy Is Not as Hard as You Might Think. Consumer Reports. Retrieved online on September 20, 2016 from http://www.consumerreports.org/privacy/protecting-your-digital-privacy-is-not-as-hard-as-you-might-think/

[2] Arvidson, E. "What Are the Concerns With Cell Phone Privacy." eHow. Retrieve online on March 13, 2014 from http://www.ehow.com/print/info_8244653_concerns-cell-phone-privacy.html

[3] Bélanger, F., &Crossler, R.E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly, 35 (4): 1017-1041.

[4] Consumer Reports (September 20, 2016). Where Consumer Reports Stands on Privacy Issues: Individuals Should Be Able to Exercise Choice and Control Over the Use of Their Data. Retrieved online on September 20, 2016 from http://www.consumerreports.org/privacy/where-consumer-reports-stands-on-privacy-issues

[5] Dinev, T.,&Hart, P. (2006). Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use. E-Service Journal, 4 (3): 25-59.

[6] Fuscaldo, D. (2016). Yahoo Data Breach May Impact AT&T (T, YHOO). Investopedia – Retrieved online on September 27, 2016 fromhttp://www.investopedia.com/news/yahoo-data-breach-may-impact-att-t-yhoo/#ixzz4LZKT5M7A

[7] Griffin, A. (2016). Yahoo hack: Hundreds of millions of people probably don't know they are part of the world's biggest data breach. The Independent – Retrieved online on September 28, 2016 from http://www.independent.co.uk/life-style/gadgets-and-tech/news/yahoo-hack-flickr-account-how-to-know-what-to-do-have-i-been-hacked-data-breach-a7324701.html

[8] Hewson, K. (2013). What is the size of your digital footprint? The Phi Delta Kappan, 94 (7): 14-17.

[9] Kanter, M.,&Robbins, S. (2012). The Impact of Parents "Friending" Their Young Adult Child on Facebook on Perceptions of Parental Privacy Invasions and Parent–Child Relationship Quality. Journal of Communication, 62 (5): 900–917

[10] Kennedy-Lightsey, C.D.,&Frisby, B.N. (2016). Parental Privacy Invasion, Family Communication Patterns, and Perceived Ownership of Private Information. Communication Reports, 29(2):75-86.

[11] Kehr, F., Kowatsch, K., Wentzel, D., &Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Information Systems Journal, (25): 607–635

[12] Li, T., &Slee, T. (2014). The Effects of Privacy Information Concerns on Digitizing Personal Health Records. Journal of the Association for Information Science and Technology, 65(8): 1541-1554.

[13] Libert, T., Grande, D.,&Asch, D. (2015). What your digital footprint reveals about your health. British Medical Journal (BMJ BR MED J), 351(8037): h5974-2.

[14] McBride, C.,&Bergen, K. (2008). Communication Research: Becoming a Reluctant Confidant: Communication Privacy Management in Close Friendships,Texas Speech Communication Journal, 33 (1): 50–61.

[15] Miller, S.,&Weckert, J. (2000). Privacy, the Workplace and the Internet. Journal of Business Ethics, 28 (3): 255–65.

[16] Ngcongo, M. (2016). Mobile communication privacy management in romantic relationships: a dialectical approach. Communicatio: South African Journal for Communication Theory & Research, 42 (1): 56-74.

[17] Osatuyi, B. (2014). An Instrument for Measuring Social Media Users' Information Privacy Concerns. Journal of Current Issues in Media & Telecommunications, 6(4): 359-375.

[18] Pervasive Computing. Webopedia – Retrieve online on September 28, 2016 from http://www.webopedia.com/TERM/P/pervasive_computing.html

[19] Perlroth, N. (2016). Yahoo Says Hackers Stole Data on 500 Million Users in 2014. The New York Times – Retrieved online on September 22, 2016 from http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html?_r=0

[20] Petronio, S. (2013). Brief Status Report on Communication Privacy Management Theory. Journal of Family Communication, 13: 6–14.

[21] Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between married couples. Communication Theory. 1: 311–335.

[22] Privacy Rights Clearinghouse (March 13, 2014). Fact Sheet 2b: Privacy in the Age of the Smartphone. Retrieved online on May 2, 2014 from https://www.privacyrights.org/print/smartphone-cell phone-privacy

[23] Quinn, K. (2016). Why We Share: A Uses and Gratifications Approach to Privacy Regulation in Social Media Use. Journal of Broadcasting & Electronic Media, 60(1): 61–86

[24] Riley v California, 573 U. S. ____ (2014)

[25] Satyanarayanan, M. (2001). Pervasive Computing: Vision and Challenges. IEEE PERSONAL COMMUNICATIONS, 8(4): 10-17

[25] Shilton, K. (2009). Four BillionLittle Brothers? Privacy, Mobile Phones, and Ubiquitous Data Collection. Communications of the ACM, 52(11): 48-53.

[27] Stewart, K.A., &Segars, A.H. (2002). An empirical examination of the concern for information privacy instrument. Information Systems Research, 13(1): 36-49.

[28] Such, J.M.,&Rovatsos, M. (2016). Privacy Policy Negotiation in Social Media. ACM Transactions on Autonomous and Adaptive Systems, 11(1): 4.2-4.28

[29] Vik, T.A.,&Bates, B.R.(2016). Disclosure without Boundaries: Examining Communication Privacy Management theory in a Counterfactual World. Journal of the Communication, Speech & Theatre Association of North Dakota, (28):48-62

[30] Xu, H., &BéLanger, F. (2013). Information Systems Journal Special Issue on: Reframing Privacy in a Networked World. Information Systems Journal (23): 371-375.

[31] Youn, T., Kim, J., & Lim, M. (2014). Study on two privacy-oriented protocols for Information Communication Systems. Journal of Intelligence Manufacturing, 25:339–345

[32] Zhang, J.,Li, H.,&Luo, X. (2016). Exploring the Effects of the Privacy-Handling Management Styles of Social Networking Sites on User Satisfaction: A Conflict Management Perspective, Decision Sciences. 00(0): 1-34.