Interested in learning more about security?

SANS Institute InfoSec Reading Room

Legal Aspects of Privacy and Security: A Case-Study of Apple versus FBI Arguments

The debate regarding privacy versus security has been going on for some time now. The matter is complicated due to the fact that the concept of privacy is a subjective phenomenon, shaped by several factors such as cultural norms or geographical location. In a paradoxical situation, rapid advancements in technology are fast making the technology both the guardian and invader of the privacy. Governments and organizations around the globe are using technology to achieve their objectives in the name of security and conveni...

Legal Aspects of Privacy and Security: A Case-Study of Apple versus FBI Arguments

GIAC (GLEG) Gold Certification

Author: Muzamil Riffat, muzamil@hotmail.com
Advisor: Chris Walker
Accepted: June 1, 2016

Abstract

The debate regarding privacy versus security has been going on for some time now. The matter is complicated due to the fact that the concept of privacy is a subjective phenomenon, shaped by several factors such as cultural norms or geographical location. In a paradoxical situation, rapid advancements in technology are fast making the technology both the guardian and invader of the privacy. Governments and organizations around the globe are using technology to achieve their objectives in the name of security and convenience. It appears that sporadic fights of the proponents of privacy and security had eventually found an avenue to express their opinions i.e. the USA court system. In February 2016, FBI was able to obtain a court order requiring Apple to modify the security features of an iPhone to enable the law enforcement agency access the contents of the device. Apple, backed by other leading technology firms, had vehemently opposed the idea and intended to file a legal appeal against the court order. Before both parties could present their arguments in the court, the case was dropped by FBI as it claimed that it was able to access the contents of the device without Apple's assistance. By using FBI vs. Apple as a case-study, this paper discusses different legal aspects of the opinions of both parties. With the pervasiveness of advanced technology, it can be reasonably anticipated that such requests by law enforcement and government agencies will become more frequent. The paper presents the privacy concerns that should be taken into consideration regarding all such requests.

1. Introduction

Some people argue that achieving absolute privacy has become synonymous with chasing a chimera. The subject matter is complicated due to the fact that there is no single universally accepted definition of what privacy really means or entails. Instead, the notion of privacy is influenced by auxiliary factors such as culture, location, use of technology and perceived benefits from information sharing. The rapid advancement in technology has certainly played a key part in further diluting the understanding of privacy. While technology has enabled a world of information to be available to us, it has also enabled information about us to be available to the world (Ahmed, 2010). The use of social media is increasing at a fast pace. As communication and information technology have evolved, Internet activities and specifically the use of social media have become mainstream (Madden, 2012). The information and communication technology advancements are happening at such a fast pace that it is hard to predict how the ocean of data humans are producing every minute will be analyzed, aggregated and utilized. The benefits the new information economy promises cannot be undervalued, but the accompanying perils cannot be underestimated either.

The situation seemingly at the opposite ends of the spectrum i.e. abundance of information at one end, and the desire to protect the information on the other end, has initiated a fierce debate about the privacy and its applicability in today's world. There are some serious concerns regarding individual data as well as aggregates arising from data mining (Cringely, 2010). Governments and privacy advocates have also moved to streamline privacy regulation and query organizations regarding their information privacy policy and practices (Angwin & Thurm, 2010).

Since the information can be used in multiple powerful ways, it is not surprising that governments and organizations are utilizing whatever methods available to them to employ data collection and analysis technologies for their noble or notorious objectives. This in turn is spraying fuel on already fired up privacy debates. The fact of the matter, however, is that the choice of privacy is slowly snatched away from the users. One decision at a time, the users are willing to surrender a little bit of privacy to reap the

perceived benefits of convenience the technology offers. The cumulative effect of these individual tradeoffs may result in complete failure of efforts to safeguard the privacy.

2. Defining Privacy

Although most people have some notion of privacy, the universally accepted definition has so far eluded academics and researchers. However, everyone seems to be concerned about and want to protect their private information. Linguistically, the term privacy seems to have been derived from the Latin word *privatus*, which means *isolated, restricted, personal* or *peculiar* (Traupman, 1995). Therefore, it can be deduced from the definition that any information that an individual wants to protect from becoming a public knowledge can fall under the realm of privacy. It is important to note that ultimately "it is the right of the individual to determine when, how, and to what extent there should be disclosure of the information" (Westin, 1967). The difficulty in defining privacy in the modern age has led to the focus on what privacy actually entails rather than what it really means. Ebenger (2004) has illustrated five legal or philosophical viewpoints on privacy. First, privacy is control over information or activities relating to oneself. Second, privacy can be considered as a "derivative" right i.e. privacy right is derived from other related rights. Third, privacy to be viewed as a tort. Fourth, the right of privacy in the light of constitution restricting unauthorized searches and seizures. Lastly, a viewpoint that privacy is not a basic requirement of our society.

2.1. Privacy as Control over Information

Each individual have a distinct lifestyle, habits, personal history, and preferences. Regardless of its source, the information should not be disclosed to a third party without the authorization of the information owner. This viewpoint stipulates that only the information owner makes the decision about the disclosure of the information. For instance, the privacy would deemed to be compromised if an employee working in a government tax office views the records of someone else out of personal interest.

2.2. Derivative Right

The idea of privacy as a derivate right has been championed by Judith Jarvis Thomson (1975). According to her, the privacy right is derived from other clusters of rights. In absence of a clear definition of privacy, any suspected case of violation of privacy should be looked form the perspective whether other intersecting cluster of rights have been violated or not. The cluster of rights provide an individual right "to do certain things to or in respect of" a thing, object, or any possession. Thomson gives an example that the act of owning a picture provides a cluster of rights such as the right to sell it, the right to destroy it, the right to view it etc. If someone looks at the picture in an unauthorized manner, the rights associated with owning the picture, specifically the right that no one else should look at it, would be violated. Therefore, she concludes, the privacy right would also be violated.

2.3. Privacy as Tort

The eminent US law scholar William L. Prosser (1960) proposed that the invasion of privacy would deem to have occurred under the following four claims:

2.3.1. Intrusion upon Solitude or Seclusion, or into Private Affairs

Intrusion upon solitude or seclusion, or into private affairs would be considered a liability if the intrusion is not acceptable to a "reasonable person". The illegal interception of phone or electronic messages would be considered a violation of privacy as these communications can be considered as private matters. Similarly, if someone uses very powerful binoculars to view a thing, object, information or a person across the window, then such an act would be associated with violation of privacy.

2.3.2. Public Disclosure of Embarrassing Facts

The legal course of action can be initiated if an individual publicly discloses truthful private information that is not in general public's interest and "the matter made public must be one which would be offensive and objectionable to a reasonable man of ordinary sensibilities" (Prosser, 1960).

2.3.3. Publicity in the False Light in the Public Eye

Any false comments or opinions that are misleading and that cause a bad reputation ("false light") can be sued for violation of privacy under this tort.

2.3.4. Appropriation of Name of Likeness for Advantage

If anyone uses the name or likeness for benefit without consent may result in plaintiff claiming damages. Usually, the celebrities claim damages under this category when an organization uses celebrity's unique claim to fame for marketing or commercially benefit purposes.

2.4. Privacy Right in the US Constitution

Although the notion of privacy as a right does not specifically appear in the US constitution, it can be deduced from the other related provisions. The amendments made to the Constitution afterwards are understood to have addressed the concerns related to protection of privacy. These are the First (speech, religion), Third (quartering soldiers), Fourth (against seizure and searches), Fifth (against self-incrimination), Ninth (for general liberties) and Fourteenth (for personal liberty versus state action) amendments (Nissenbaum, 2004). The Fourth Amendment is considered to be most close to the concept of privacy as we understand today. The Article IV of the Amendment states, "The right of the people to be secure in their persons, houses, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

There are a few important elements within the text of the Article IV of the Fourth Amendment that must be disentangled to fully understand the intention behind the amendment. Firstly, the provisions contained within the Fourth Amendment address any violation by government only. Therefore, legal protection cannot be sought if the material searched or seized is by other individual, groups, corporations, or an Internet Service Provider (Ebenger, 2004). Secondly, the citizens are protected from *"unreasonable"* searches and seizures. However, an explicit definition of what constitutes an unreasonable action has not been mentioned. Thirdly, a warrant must be obtained before

search or seizure action can be carried out by the government. The warrant could only be granted if there is a "probable cause". Again, the elaborate and specific scenarios that might create a probable cause are not defined. Due to the subjective interpretation of the law, it is not entirely surprising that in the age of modern information and communication, the expectations of privacy under the Fourth Amendment can vary significantly. Different courts, depending upon the context of the case, might give a conflicting opinion in seemingly similar situations. Another critical element contained within the Fourth Amendment is the "inside/outside" heuristic. In the court ruling of the classic case *Katz v. United States (1967)*, Justice Harlan determined that government requires the warrant with probable cause only in cases where the search or seizure needs to be carried out in a closed space. In public areas, however, it would be unreasonable for a person to expect privacy. Therefore, according to Justice Harlan, the government is allowed to use any material or evidence that is in public view. Justice Harlan further concluded that not necessarily everything that is within a closed space would trigger the Fourth Amendment protection. Similarly, not everything in public would be exempted from the protection. For instance, Justice Harlan found the government to be in violation of the Fourth Amendment when the police agents eavesdropped and monitored telephone calls made from a public telephone. The court ruling is important in the aspect that it shifted the premise of privacy from the space ("*outside"* or "*inside")* to the person. Therefore, if a person knowingly exposes anything to the world even from the closed boundaries of her home, it would not necessarily provide protection under the Fourth Amendment. Similarly, if a person seeks to preserve some information private, even in the public space, the information would be constitutionally protected. Thus, according to the Supreme Court judgement, "the reasonable expectation of privacy has two requirements: first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable"". Although *Katz case* can be termed as a triumph for advocates of privacy, it has opened a Pandora's Box for other such cases. In the cyber security world, an individual launching a malicious attack from a public internet provided by a café or airport might claim protection under the Fourth Amendment if the law enforcement organizations try to seize her computer. More likely than not, the computer used in the

perpetrated crime would be password protected (an exhibition of expectation of privacy), and the society in general would find such expectations to be reasonable.

In addition to different amendments in the Constitution, the privacy right has been given due considerations through specific acts pertaining to specific areas. For example, student information is protected through Family Education Rights and Privacy Act of 1974, financial information through Right to Financial Privacy Act of 1978, health information through Health Insurance Portability and Accountability Act of 1996, and electronic transmissions through Electronic Communications Privacy Act of 1986.

In Europe, where the privacy laws are considered to be more stringent, European Directive 95/46/EC, known as the Data Directive, imposes restrictions and requirements on the collection and use of data belonging to European citizens (Korba, 2002).

2.5. Privacy… No, Thanks

Some people question whether privacy is actually a basic human right. The typical argument given is that if one has nothing to hide, one should not be fearful if any so-called private information is collected. The argument is raised more so in the case of mass surveillance performed by the governments. The opponents of privacy contend that one of the primary responsibilities of the government is to provide security to its citizens. The endeavors to provide security necessitate a mass surveillance mechanism in the modern world. The argument is further enforced by stating that the only person who would be concerned by monitoring activities is the one who is engaged in any illegal or unauthorized activity. For instance, if someone is only visiting legitimate websites at work, the employee should not be concerned about how the information about the web browsing activity is monitored or recorded. Privacy advocates have challenged the "nothing to hide, nothing to fear" idea in more than one way. They proclaim that the idea assumes complete trust in the authority who is collecting or monitoring the data in a sense that the private information in their possession would only be used for catching any illegal activity and not in any other deceitful manner. There is no guarantee that such assumption would always hold true. Another counter argument is that the privacy is rarely lost in absolute terms through only one action. If the mass surveillance system is

set-up just to monitor the internet browsing habits, it might not raise a lot of concerns. However, combine that with monitoring of phone calls, surveillance in public areas through cameras, ability and authority to obtain bank records, and access to health-related information, only then one begins to wonder if their life has become an open book with the government having access and knowledge of each page.

3. Privacy Considerations

This section covers a few areas of our day-to-day life that might be deemed significant from privacy perspective.

3.1. E-mail

E-mail has become a de-facto mode of communication for both personal and professional needs. The increased usage of e-mail has been epitomized by US President Barack Obama using a hand-held device to communicate via email. The perceived insecure usage of e-mail also attracted controversy when Hillary Clinton, in a position of Secretary of State, set-up a personal e-mail server to communicate for official purposes. Most websites use the e-mail address as the identity information. The communication in the office environment cannot be imagined without the use of e-mail. Although the use of social media is presenting challenges to e-mail usage for personal matters, e-mails are still frequently used to remain in touch with family and friends.

Given the ubiquitous presence of e-mail systems, it is naturally a target of information security hackers and viruses. All such attacks either try to steal confidential information contained within the e-mail messages or use e-mail as a tool to launch other types of attacks e.g. Phishing attacks etc. Melissa virus (1999) and Love Bug (2000) viruses are the examples of viruses that spread through e-mail and caused heavy damage to many organizations.

The intention of sending an e-mail message is that the message will be delivered to the unique destination address(es), and the confidentiality and integrity of the message would be maintained. The internet serves as the conduit through which global e-mail network operates. Before reaching the recipient mailbox, the message travels through

intermediate devices and leased lines, known as hosts and routers, which are often operated and owned by third parties (O'Brien, 1999). A copy of the message might be stored in several devices as it passes through the origin device and server, to destination server and device. This so-called "store-and-forward" technology might be necessary for technical reasons but raises serious privacy concerns on the part of users (Rest, 1998). From a law enforcement perspective, there is a challenge to detect and prevent e-mail usage for illegitimate and unauthorized purposes. Detection and prevention of these activities entail invading the privacy of citizens by accessing and sometimes monitoring their emails (Guirguis, 2001). However, the balance needs to be maintained so that the right of privacy in e-mail communication is not unreasonably compromised if the law enforcement agencies are allowed indiscriminate searches of private e-mails. The right of privacy in the case of e-mail should be maintained as mentioned in the Fourth Amendment.

A US law enforcement agency came under fierce attack from the privacy advocates when it was disclosed in the year 2000 that a custom-built program named "Carnivore" was designed and implemented for reading e-mails and other online communications. The program was later renamed as DCS-1000. Under intense scrutiny and outcry, the government agency declared in 2005 that it was abandoning the use of the program altogether. However, according to the documents leaked by the US contractor whistleblower Edward Snowden, the government has implemented a program called "PRISM" that authorizes, among other things, the monitoring of e-mails without obtaining a warrant. The acknowledgment of the existence of the PRISM program has again ignited debate about privacy versus security.

From the legal protection perspective, Electronic Communication Privacy Act (1986) provides privacy safeguards for Internet communications. The ECPA contains two titles: Title I is "Wire and Electronic Communications Interception and Interception of Oral Communications" (§ 2510, et. seq.) and Title II is "Stored Wire and Electronic Communications and Transactional Record Access" (§ 2701, et. seq.). The section 2511 of Title I considers that anyone (government or a private party) would be performing a criminal act for interception, disclosure, or usage the contents of illegally obtained wire, oral, or electronic communications. The Title II, commonly known as "The Stored

Communications Act", provides protection of communications during transmission. The ECPA has provisions for exceptions for the service providers or lawful access by government entities. Just like in other technological related laws, ECPA does not provide absolute privacy protection (Ebenger, 2004). In different court cases, the provisions of ECPA have been interpreted differently depending upon the context of the particular case. One of the nuisances of using e-mail is receiving unwanted marketing or spam e-mails. The CAN-SPAM Act of 2003 defines standards that need to be followed for sending commercial e-mails. The three major areas addressed in the act are: provisions for unsubscribing that should be honored within ten business days, the compliance with defined set of rules for content, and the compliance with the defined sending message behavior.

3.2. Social Networking Sites

With the proliferation of networking sites, the use of social media has become mainstream (Madden, 2012). However, social networking sites present a paradoxical dilemma from the privacy perspective. Some people take the view that if a user is publishing her details on a social networking site, then implicitly the desire of reasonable level of expectations of privacy is naturally forfeited by the very act of putting the details on a public website. Others argue that even in the usage of social networking sites lay the basic privacy requirements, and users use the privacy settings of the social networking site to balance the competing desires of privacy and publicity (Metzger & Pure, 2009). Furthermore, they make an argument that most users do not fully comprehend about how their data is stored, used and analyzed, and therefore it would be unreasonable to assume that just by joining a social networking site and by posting messages on it, the users have agreed to surrender their right of privacy for their personal data (Boyd, 2010). The body of case law in the area of Internet-related technology "is still relatively sparse, and only a handful of courts have had occasion to grapple with the rapidly evolving nature of privacy within social networking sites" (Pure, 2013). In determining the outcome of the cases, the courts have predominantly relied on the notions of "reasonableness" and "proportionality". As demonstrated in *Katz v. United States* case, the courts typically

judge the reasonableness on two counts: First, an assessment whether a person had a subjective expectation that the information would remain private at the time it was disclosed. Second, would the public consider that expectation as reasonable? In the absence of empirical data about public's expectation of privacy, the judges have to make a subjective decision in the context of the case presented as well as the technological understanding at the time of the court case. Given the rapid advancement in technology and fluid understanding of privacy, the courts might render conflicting decisions within a short span of time.

There are primarily two main privacy mechanisms used in social network sites i.e. social networking site's privacy settings and the privacy policies of the platform. The privacy settings typically protect users' information from other users. The privacy policies dictate how the data about the users would be protected or shared with external parties. Due to different understandings of the privacy and technological changes, some judges took a position that regardless of privacy settings, postings on the social networking sites do not warrant reasonable expectations of privacy due to public nature of the platform (Romano v. Steelcase, Inc., 2010). Other judges took into consideration the privacy settings and deemed the information posted on social media sites to be private (Crispin v. Christian Audigier, Inc., 2010). The profile of a user might contain information such as name, gender, age, location, and hobbies etc. Although most people try to restrict the information through applying privacy settings, many users might have a public profile due to personal choice or due to lack of adequate skills in applying the privacy settings (Tufekci, 2008). For instance, a study performed by Ralph Gross, Alessandro Acquisti, and H. John Heinz, III on the usage of privacy settings of the popular networking site Facebook revealed that most users do not change the default privacy settings, and therefore their information is not adequately protected from strangers. Furthermore, a substantial amount of personal information can be harvested through multiple social networking sites that can then be used in social phishing attacks (Jagatic et al., 2007).

With the popularity and usage of social media growing at an unprecedented rate, the concerns related to privacy have to be addressed at multiple levels. The social awareness has to be enhanced about the risks of posting private information on such

platforms. In addition, the technical controls in the protection of information need to be reassessed and reconfigured to more stringent requirements. Lastly, the laws and legal frameworks need to be enhanced to address the ever-changing technological landscape and the services offered by the social networking sites.

4. Apple vs. FBI – Case Study

In the recent past, nothing has captured the attention of the world more than the tussle between the technology company "Apple" and the US law enforcement agency "FBI". The legal battle focused on two aspects: the perceived privacy and the deemed security for the citizens. Upon the request of FBI, a court order was issued to Apple in February 2016 to assist in circumventing the security measures of a device used by a terrorist. Without bypassing the security controls, FBI was not able to access the contents of the device. Apple's refusal to comply triggered a fierce debate about the security and privacy. Some people argued that by not complying with the court order, Apple broke the law. However, in other people's opinion, Apple had the right of appeal against the court order, and the company could only be enforced to follow the court order if all possible avenues of appeal have been exhausted. If both parties stood their ground and engaged in the lengthy court proceedings, then the final decision would be made by the Supreme Court that would be binding on both parties.

Since the body of law surrounding technology in general and privacy in specific is murky, Apple and other companies supporting its stance believed that the law enforcement agency is attempting to set a "precedent" for accessing encrypted and private information. According to Wikipedia definition, "a precedent is a principle or rule established in a previous legal case that is either binding on or persuasive for a court or other tribunal when deciding subsequent cases with similar issues or facts". In Apple's opinion, the desire to create a computer program that would alter the technical controls implemented for the protection of information amount to creating a back-door that could also be used by the hackers to compromise the security of devices used by other customers. Furthermore, analysts point out that if Apple complied with the request, it would set a dangerous precedent and it will be harder for the company to refuse any such requests in future. Apple also feared that if it complied with the request in one country, it

would be difficult for the company to not comply with similar requests in other countries where the human rights and civil liberties are not at the acceptable international standard. Apple insisted that creation of the custom program as desired by FBI would result in the violation of principles behind Fourth Amendment. Some industry experts also questioned the notion that only Apple has the extensive technical expertise to break into the device. Theoretically, a process known as "Decapping" might allow recovering the cryptographic keys from the device by physical intervention in the transistors and other micro hardware elements. This kind of work can only be performed by a few dedicated and specialized organizations. However, if the criticality of obtaining information were to be so essential, the possibility to take such an action certainly exists.

A key question to consider in this legal battle is whether FBI's request fulfilled the criterion of "proportionality" i.e. was the effort required to bypass the security controls of the device, as well as the eventual ramifications, proportional to the usefulness of the information that could be obtained from the device? FBI certainly thinks so. In FBI's opinion, the information obtained from a device used by the terrorist could provide valuable clues and links regarding the terrorist network, thereby diminishing the probability of more attacks on the citizens. Furthermore, the request to bypass the security controls was directed towards a specific device that uses an outdated operating system. In FBI's opinion, it would be very hard to apply the same technique to devices with an updated operating system. In addition, the phone was not a privately owned device. Instead, it is owned by the government department where the terrorist was employed. Therefore, the law enforcement agency had the right to request access to the contents of the device as it would be requesting access to information on a government owned asset.

Before the above mentioned contrasting arguments could be presented to the court, FBI requested to drop the case by stating that it managed to access the contents of the device without Apple's assistance. Till date, FBI has neither released the technical details of how the access was made possible, nor the information about any third-party that might have aided FBI. On the surface, it might seem that the issue has been resolved. However, a deeper introspection indicates that a similar case is bound to arise again. There are three main considerations that need to be taken into account for such cases in

future. First, the technology companies will deliberately try to modify the security mechanism of their devices such that it would be impossible to access the contents of the device, even with a custom created computer program. For instance, the newer versions of Apple's iPhone have a separate computer to monitor the access to the device. This separate computer is called "Secure Enclave". Currently Apple has access to modify the security controls of Secure Enclave. However, in future Apple might decide to build the architecture in a way that even Apple would not have the capability to modify the functionality of the separate computer monitoring the access to the device. In that case, it would be virtually impossible for Apple to fulfill any requests from authorities to circumvent the access controls. Secondly, it has now become public information that security of the specific model of iPhone can be compromised as FBI has publicly stated that it has managed to gain access to the device used by the terrorist. Apple will certainly be interested in knowing the details of that vulnerability and providing a security update to its system in order to close the hole. It will be interesting to observe if Apple would decide to file a court request forcing FBI to reveal the details of the vulnerability exploited in order to protect millions of other similar devices used by the general public. Lastly, will government move in the direction of creating legislation where it would be mandatory for the technology companies to keep a back-door? The access to information is a fundamental component if the security needs to be provided to the citizens. If the technology companies and advocates of privacy do not agree with creating back-doors, then they must propose a solution acceptable to the law enforcement agencies in fulfilling the mandate of providing security services to the citizens.

5. Conclusion

The concept of privacy is very fluid, and the laws related to this topic are murky and subjective. Despite numerous attempts by many scholars, the universally acceptable definition of privacy has been elusive. The rapid pace of technology development is having an unprecedented impact on our understanding and acceptability of protection of private information or lack thereof. Some pundits declare that "the right to be left alone" has been snatched from the citizens in the name of security or convenience. Due to the perceived benefits of technology, users are willing to sacrifice a little bit of privacy for

the convenience offered by the technological products. The cumulative impact of all these trade-offs results in complete erosion of privacy. The current geopolitical and social situation has brought security as the main concern for the citizens of any country. The governments around the world have responded to this concern by enhancing their mass surveillance programs. The kind of personal information that is collected through mass surveillance programs ignites a fierce debate between the advocates of privacy and security. The rise of social media and other social networking sites have resulted in users voluntarily or involuntary disclosing private information to the public. In the court cases, the judges have to grapple with the subjective notion of privacy, the ever-evolving technology and seemingly outdated legislations to make a decision. Since information is power, governments and organizations are trying their best to maximize data collection to achieve their objectives. As has been demonstrated by the recent case involving FBI and Apple, the demands by the law enforcement agencies to gain access to private information will only grow as more advanced technology is developed. It can be reasonably anticipated that the notion of privacy will become more complex in the near future as the technology will provide more avenues for collecting, sharing and analyzing personal information. The court rulings in legal cases related to privacy will also become more subjective, confusing and contradicting.

References

Ahmad, A. (2010). *The effect of perceived privacy breaches on continued technology use and individual psychology: The construct, instrument development, and an application using internet search engines,* Available from ProQuest Dissertations & Theses Full Text: The Humanities and Social Sciences Collection (Order No. 3440262)

Angwin, J. & Thurm, S. (2010). *Privacy defense mounted*. The Wall Street Journal. October 8. Available: http://online.wsj.com/article/SB10001424052748704011904575538372505294514.html

Boyd, d. (2010). "Why youth (heart) social network sites: The role of networked Publics". In D. Buckingham (Ed.), Youth, identity, and digital media (pp. 119-142). Cambridge, MA: MIT Press.

Conboy, K. (2010) *Project failure en masse: a study of loose budgetary control in ISD projects*, European Journal of Information Systems, 19(3), 273-287.

Cringely, R. (2010). "*Online Advertisers Are Selling You Out*", PC World, Oct 25. Available: http://www.pcworld.com/article/208741/online_advertisers_are_selling_you_out.html

Ebenger, T. (2004). *Privacy, technology and public policy: The case of electronic mail.* Available from ProQuest Dissertations & Theses Full Text: The Humanities and Social Sciences Collection (Order No. 3252725)

Muzamil Riffat, muzamil@hotmail.com

Guirguis, M. (2001). "*Privacy in the dawn of a new age: A study of the legal and moral limits on high-tech government surveillance".* Available from ProQuest Dissertations & Theses Full Text (Order No. 3028863).

Jagatic, T, Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer, *Social phishing, Communication.* ACM 50 (2007), no. 10, 94-100. 26

Korba, L. (2002). "*Privacy in distributed electronic commerce".* Proceedings of the 35th Hawaii International Conference on System Science (HICSS), Hawaii. January 7-11

Madden, M. (2012). *Privacy management on social media sites*, Pew Internet & American Life Project, 24

Metzger, M. J., & Pure, R. A. (2009). *Privacy management in 'facebook': An application and extension of communication privacy management theory to online social networking.* Paper presented at the 95th Annual National Communication Association Convention, Chicago, IL.

Nisseanbaum, H. (2004). "*Privacy as contextual integrity".* Washington Law Review 79, 119-158.

O'Brien, M. Sean (1999) "*Extending the Attomey-Client Privilege: Do Internet Email Communications Warrant a Reasonable Expectation of Privacy*?", Suffolk Journal of Trial & Appellate Advocacy, 187

Prosser, William L. (1960). "*Privacy*" California Law Review, 48 (1960): 338-423

Pure, R. A. (2013). *Privacy expectations in online contexts* (Order No. 3602192). Available from ProQuest Dissertations & Theses Full Text: The Humanities and Social Sciences Collection.

Muzamil Riffat, muzamil@hotmail.com

Rest, L. Colleen (1998). *"Electronic Mail and Confidential Client-Attomey Communications: Risk Management,"* Case Western Reserve Law Review vol. 48 (Winter 1998): 315

Thomson, Judith (1975). "*The Right to Privacy*" Philosophy and Public Affairs, Vol. 4, No. 4 (Summer, 1975)

Traupman, John C. (1995) "Privatus" The New College Latin and English Dictionary. (New York: Bantam books, 1995)

Tufekci, Z. (2008). *Can you see me now? Audience and disclosure regulation in online social network sites*. Bulletin of Science, Technology & Society, 28(1), 20-37.

Last Updated: September 19th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Rocky Mountain Fall 2017	**Denver, COUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Baltimore Fall 2017	**Baltimore, MDUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
Data Breach Summit & Training	**Chicago, ILUS**	**Sep 25, 2017 - Oct 02, 2017**	**Live Event**
SANS Copenhagen 2017	**Copenhagen, DK**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London September 2017	**London, GB**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Oslo Autumn 2017	**Oslo, NO**	**Oct 02, 2017 - Oct 07, 2017**	**Live Event**
SANS DFIR Prague 2017	**Prague, CZ**	**Oct 02, 2017 - Oct 08, 2017**	**Live Event**
SANS Phoenix-Mesa 2017	**Mesa, AZUS**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS October Singapore 2017	**Singapore, SG**	**Oct 09, 2017 - Oct 28, 2017**	**Live Event**
Secure DevOps Summit & Training	**Denver, COUS**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS Tysons Corner Fall 2017	**McLean, VAUS**	**Oct 14, 2017 - Oct 21, 2017**	**Live Event**
SANS Brussels Autumn 2017	**Brussels, BE**	**Oct 16, 2017 - Oct 21, 2017**	**Live Event**
SANS Tokyo Autumn 2017	**Tokyo, JP**	**Oct 16, 2017 - Oct 28, 2017**	**Live Event**
SANS Berlin 2017	**Berlin, DE**	**Oct 23, 2017 - Oct 28, 2017**	**Live Event**
SANS Seattle 2017	**Seattle, WAUS**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
SANS San Diego 2017	**San Diego, CAUS**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
SANS Gulf Region 2017	**Dubai, AE**	**Nov 04, 2017 - Nov 16, 2017**	**Live Event**
SANS Miami 2017	**Miami, FLUS**	**Nov 06, 2017 - Nov 11, 2017**	**Live Event**
SANS Milan November 2017	**Milan, IT**	**Nov 06, 2017 - Nov 11, 2017**	**Live Event**
SANS Amsterdam 2017	**Amsterdam, NL**	**Nov 06, 2017 - Nov 11, 2017**	**Live Event**
SANS Paris November 2017	**Paris, FR**	**Nov 13, 2017 - Nov 18, 2017**	**Live Event**
Pen Test Hackfest Summit & Training 2017	**Bethesda, MDUS**	**Nov 13, 2017 - Nov 20, 2017**	**Live Event**
SANS Sydney 2017	**Sydney, AU**	**Nov 13, 2017 - Nov 25, 2017**	**Live Event**
SANS London November 2017	**London, GB**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CAUS**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SIEM & Tactical Analytics Summit & Training	**Scottsdale, AZUS**	**Nov 28, 2017 - Dec 05, 2017**	**Live Event**
SANS Khobar 2017	**Khobar, SA**	**Dec 02, 2017 - Dec 07, 2017**	**Live Event**
SANS Munich December 2017	**Munich, DE**	**Dec 04, 2017 - Dec 09, 2017**	**Live Event**
European Security Awareness Summit 2017	**London, GB**	**Dec 04, 2017 - Dec 07, 2017**	**Live Event**
SANS Austin Winter 2017	**Austin, TXUS**	**Dec 04, 2017 - Dec 09, 2017**	**Live Event**
SANS Frankfurt 2017	**Frankfurt, DE**	**Dec 11, 2017 - Dec 16, 2017**	**Live Event**
SANS Bangalore 2017	**Bangalore, IN**	**Dec 11, 2017 - Dec 16, 2017**	**Live Event**
SANS SEC504 at Cyber Security Week 2017	**OnlineNL**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**