Issues in Information Systems
Volume 19, Issue 1, pp. 83-90, 2018

PERCEPTION OF PRIVACY THROUGH GENERATIONS

Xavier Aguirre, Southern Illinois University, xavier.aguirre66@siu.edu
Belle Woodward, Southern Illinois University, bellew@siu.edu
Nancy Martin, Southern Illinois University, nlmartin@siu.edu

AUTHOR NOTE

This research was supported in part by the McNair Scholars Program at Southern Illinois University.

ABSTRACT

This is study is an exploration into the perception of privacy among various age groups. The study utilized a qualitative approach with focus groups and one-on-one interviews. There was a total of 20 participants between the ages of 18 and 63. The data revealed four recurring themes: (1) Young adults were less concerned with companies having their information than older adults, (2) All study participants take precautions to protect privacy, (3) All subjects have a consistent misunderstanding of technology and online privacy, and (4) All participants displayed a lack of knowledge but desire to know more about privacy rights.

Keywords: Information Technology (IT), Perceptions, Data Privacy, Generations

INTRODUCTION

The purpose of this study is to explore differences in concerns and knowledge levels among different age groups in regard to online privacy. "[Young adults] are more likely to believe that the law protects them both online and off. This lack of knowledge in a tempting environment, rather than a cavalier lack of concern regarding privacy, may be an important reason large numbers of them engage with the digital world in a seemingly unconcerned manner" (Hoofnagle 2010, 20). Younger adults do not understand the ramifications that accompany their actions online. There are some that believe they will be fine, while others are completely naïve to the lack of privacy (Marreiros, et al., 2015). In this study, the authors explore the ways in which different age groups protect their online privacy, as well as their knowledge of online privacy. This exploration is done by using focus groups and one-on-one interviews. By understanding what perceptions individuals have towards privacy, we can identify what knowledge gaps exist, and better educate ourselves and others to protect our privacy.

A literature review follows that focuses on the loss of, perceptions of, and reactions towards privacy as well as the misconceptions about technology. Following the literature review, the study methodology and results are reported. The next sections discuss the results and limitations and conclude the paper.

LITERATURE REVIEW

Loss of Privacy

Internet privacy is an ever-increasing concern for many citizens given the prevalence of online threats, private and governmental tracking, and cyber attacks by hackers. Previous studies have examined the varying levels of online privacy that individuals believe they possess as internet users. Halperin and Dror (2016) conducted a study among different generational age groups to determine how they relate to technology. Their findings show that online privacy is viewed as passé or non-existent in today's society. Their findings also show that people are willing to divulge more information than in previous years (Halperin & Dror, 2016).

Technological advances have made it possible for private and government entities to engage in constant surveillance of private citizens. This, in turn, has led to the acceptance that citizens can no longer expect laws that regulate online privacy to protect their information. Doughty (2014) discusses how there is more acceptance that there is no privacy, stating that future generations will no longer know what it is like to have privacy.

During an investigation into smartphone application breaches, Mamonov and Benbunan-Fich (2015) found that individuals do care about their privacy. However, when comparing specifics, individuals care less about information related to their location than financial information (Mamonov & Benbunan-Fich, 2015). Individuals want privacy; however, social media's content sharing capabilities have made it difficult to keep personal information private. "Most users indicate that they are concerned about their privacy, yet they share personal information widely on social media platforms" (Zurbriggen, Hagai, & Leon, 2016, 248). Individuals crave the constant attention social media provides. Ritvo (2012) examines the impact of social approval on the human brain by observing the physiological reaction to interactions on social media platforms. The findings show that the human brain releases measurable amounts of dopamine when individuals "like" posts and share information on the internet. Many individuals have become addicted and crave the constant rush of these interactions and chemical releases. Between oversharing information and cellular devices collecting information, there is a huge amount of personal information being lost; especially when data breaches occur and this data is stolen.

Perceptions and Tradeoffs of Privacy

So far, most research has shown that people do claim to care about their privacy; however, they may not care enough. Zinta et al. (2016) reported that when comparing the perception of risk associated with certain online tasks to their actual risk, generally, the levels were at odds. For instance, users perceived using Craigslist as riskier than clicking on a link within an email. However, often, links in the email are redirected to illegitimate sites that collect information from the user such as cookies and browsing history. This stems from a combination of misunderstanding, misinformation and the privacy calculus. The privacy calculus (Zinta et al., 2016) is a way of measuring the necessary privacy invasion compared to the worth of the technology. Research shows that individuals will try to divulge the least amount of information for any application (Zinta et al., 2016). The researchers also found that the usefulness of email greatly outweighs the potential danger, even though many individuals, mainly older, click on spam emails under the assumption that the link is from a legitimate source. "Overall, our results suggest that people do perceive some Internet actions as riskier than they do others, but continue to engage in them apparently for the benefits they perceive these actions provide" (Zinta, et al., 2016, 463). Individuals can recognize the dangers some sites pose, yet return to said sites for the perceived benefit.

Younger generations also need to be aware that willingly putting so much information online could lead to a higher "risk of being a victim of crime, such as burglary or online stalking which could turn into physical stalking or even harassment" (Diane, & Lily, 2015, 88). Often images are uploaded with a location attached. This is called geolocation and could show, for example, where and when someone is at the mall; someone else could take advantage of this information. For example, this knowledge could lead to their home being robbed, or someone could go to the mall and stalk them. However, such criminal behavior is hardly a thought until it occurs. The same mindset can be seen with regards to identity theft. Many people believe that it will not happen to them, so they do not take any precautions. "[W]e are complicit because we are careless about giving away our identities, and our privacy, every time we engage in social media or go shopping online" (Kirk, 2014, 449). During the moment of posting, young adults do not think about the ramifications the post may cause, only the "like" count.

The Effects of Little Privacy

As we grow with technology, we become more accustomed to it. We, as a society, want the latest and greatest that technology has to offer. There are many early adopters of smart watches and virtual reality headsets. Often at the behest of our privacy and even with a lack of understanding, we continue to consume. However, as previously stated, many users claim to care about privacy to some extent. Individuals will not freely give their email passwords to anyone that asks. Most individuals will shut their doors to their home and to their bedroom even if no one is home. There is a level of privacy most people have and continue to follow even when no one is around. If we truly do not care about our privacy, then we would not have passwords or doors in general. Some would argue that if you have nothing to hide, then you should not care if the government is reading your emails. However, our behavior changes when the possibility of us being watched is present.

At Newcastle University in 2011, an experiment was conducted on cycle thefts in certain areas on campus. The experiment consisted of adding a picture above a bike rack with "Cycle thieves we are watching you" above a set of eyes and the police logo below. For 12 months, this sign remained on the wall with no other changes or additional security. After the 12 months, they found that the number of bikes stolen from 2010 to 2011 had dropped by 62% (Nettle, Nott, Bateson, 2012). By being reminded of the potential of being watched, criminals were deterred from stealing at these locations. This relates to privacy because we all have something to hide regardless of how small. The sheer fact that we have social norms is indicative that we adjust to the public perception of "normal." Knowing that anything we send online could be seen by unknown eyes could change the way we behave. Perhaps it already has, and we just have not noticed yet. As we adjust our behavior when in public to ensure we are in line with social norms, how do we not know if we "play it safe" while online because we believe that some online activities are not private?

Misunderstanding of Technology

While interviewing 100 undergraduate students from the University of Southampton, it was found that there are three different types of users; the scared, the naïve, and the "meh" (Marreiros, Gomer, Vlassopoulos, Tonin, & Schraefel, 2015). In their study, they classified students into groups based on their belief about data tracking. Some were paranoid and overly concerned that everyone was monitoring everything they did. Some were naïve and did not believe that anyone was monitoring them or even gathering information about them. Finally, some individuals did not care and were apathetic, or "meh" about the whole notion of online privacy. The "meh" group is the fitted stereotype of young adults that post inappropriate pictures on social media (Marreiros, et al., 2015).

It could be difficult to educate individuals that may not want to know about the potential threats of internet use. According to Marreiros et al. (2015), a third of students in their study did not care about the threats and another third of students did not grasp the danger the internet could pose. "Experts have speculated that growing up online has made young people trust the web more than they probably should" (Kobliner, 2017, 2). Students need to learn about the drawbacks and dangers of the web. One of the greatest responsibilities of being an adult is to make informed decisions. These decisions can be impeded when it is difficult to understand what data companies are collecting. It is our responsibility to know what Google and other companies are doing with our data, and it is those organizations' responsibility to properly and plainly inform all users.

Individuals can acknowledge that there are some risky online activities as well as potential consequences associated with those activities, yet they return to said activity day after day. Some everyday actions, such as going through emails, have inherent risks to our privacy. Many individuals tend to ignore spam emails or open them out of curiosity. Many do not understand the full gravity of the potential harm spam mail has and write it off as a joke. "Unfortunately, that attitude underscores a popular yet fundamental miscalculation about the threat that spam poses to every one of us: namely the sheer destructive power of the botnets […]" (Krebs 2014, 24). A botnet is a collection of computers that have been infected by malicious software. After clicking on a link provided by an unknown sender, a virus or malware could be downloaded onto the host's computer. Afterwards, the hacker could then manipulate the infected computers to deny servers to any website via the infected computers. There is a gap in knowledge and a fundamental understanding of how the technology works. This, in turn, affects what they perceive to be a harm to their online privacy.

METHODOLOGY

When attempting to understand perceptions of online privacy, a qualitative approach was decided to be the best option. Using broad and general questions in focus group settings allowed participants to discuss online privacy openly. This enabled the researcher to delve deeper into their responses. The participants were not limited to multiple choice options; they could freely and openly express their ideas. The questions were a mixture of true false, yes or no, and Likert scale from 1-5. Whereas a quantitative study takes responses at face value, qualitative studies allow for the in-depth discussion of ideas. A focus group allows thoughts and ideas to flow and influence and change the opinions of the participants. This was apparent when many participants verbally stated they had changed their minds when someone else in the group made a valid point. Out of convenience and lack of participation, the researcher changed the focus group approach to one-on-one interviews. This still allowed the researcher to ask follow-up questions and asked for clarification on some responses.

Part of the interview questions were from a study done in 2013 by Phoenix Strategic Perspectives Incorporated (Phoenix Strategic Perspectives Inc., 2013) and are included in Appendix A. Additional true false questions were from a study by Hoofnagle et al. (2010). These true false interview questions are included as Appendix B.

A convenience sample was collected from Southern Illinois University Carbondale. Participants were solicited by posting signs around Carbondale, texting known individuals who live in the area, and inviting office employees from SIUC. As an incentive, pizza and soda were provided for the focus groups. The researcher identified himself as a McNair scholar conducting his first study. Each participant agreed to participate and signed a human subjects consent form. Interviews were recorded and transcribed by the researcher and each lasted roughly 20 minutes. Each participant was assigned a number to keep their identity anonymous.

There were 10 participants in the focus groups and 10 individual interviews for a total of 20 participants ranging from 18 years old to 63 years old. Eight of the participants were male, and 12 were female, and all were in the Southern Illinois University region. Their areas of interests also varied quite a bit. For example, some of the student respondents were from the economics (1), English (2), architecture (2), computer science (1), and hospitality departments (2).

Table 1. Demographics

	Younger	**Middle-age**	**Older**	
	(18-25)	(26-44)	(45-63)	**Total**
Male	3	1	3	7
Female	5	2	6	13
Total	8	3	9	20

RESULTS

The findings revealed several recurring themes.

- Young adults are less concerned with companies having their information than older adults.
- All subjects take precautions to protect privacy.
- All subjects have a consistent misunderstanding of technology and online privacy.
- All subjects have a lack of knowledge but desire to know more about privacy rights.

Concern with Companies Having Personal Data

One of the more prevalent themes was a trust in companies among younger adults. In this study, all eight of the younger adults (ages 18-25) believe that companies are protecting their information, and using that information to improve the companies' products. When asked if they understood how their information would be used by a company or an organization, one younger participant responded with "no, but I would like it to not be used other than for what they need it for", and many echoed a similar response. One middle aged individual stated "I sort of accept that [companies] are selling some of my information. Even if they say they don't, they probably do." On the other hand, older adults (ages 50-63) either limit their exposure to companies or organizations whether they be online or brick and mortar. One participant stated, "If it's something I am concerned with [for] a company, then, I try not to do business, or I try to find the privacy thing that says no don't send me all this stuff."

Precautions to Protect Online Privacy

When asked, "Have you ever refused to provide an organization with your personal information?", seven out of eight young adults stated, "I'm sure I have," where older adults stated something to the extent of, "Definitely! Oh absolutely." While both groups said yes, there is a different reasoning behind each yes.

Even though many young adults are willing to give their personal information, they still use password locks on their phones. There is still some level of privacy that they adhere to when using technology. On the other hand, there was one older individual who did not have a password lock on his/her phone. He/she stated, "I'm sure it's easy, but I just don't know how to do it." This shows that, while the function seems easy to enact, he/she still does not utilize the password lock. There is an inconsistency in actions to safeguard their privacy between personal information and preventing individuals from accessing their devices.

Misunderstanding of Technology and Online Privacy Rights
During the interviews, there was a consistent misunderstanding of how technology works. One of the questions was "Can companies follow your internet search history without your permission?" One participant responded with a "Yes they can! I search for products on one site and I see the ads for that same item on a different site!"; however, this is not how ads work.

A different question asked, "Do you feel confident that you have enough information to know how new technologies will affect your personal privacy?" Eighteen out of 20 participants responded "No." Younger respondents (18-25) commonly replied along the lines that "when new technology comes out, no one would know how to exploit it immediately". Older individuals (50-63) stated that they were not interested in new technology. Once again, the way they responded shows that while both agree, their reasoning differs. A middle-aged (38) individual believes that "we are losing our privacy" and we will continue to lose our privacy.

In the series of nine true-false questions regarding privacy rights, 17 of 20 participants got at least one question wrong, and 11 of 20 participants got 77% correct. Often times, respondents showed surprise when they learned the degree to which their information was exposed.

Lack of Privacy-Related Knowledge but a Desire to Know More
The questions pulled from Phoenix Strategic Perspectives (see Appendix A) were ranked on a scale of one to five, one being the lowest and five being the highest. On average, younger adults would rate their level of knowledge over privacy rights lower than older individuals (see Appendix C). Regardless of age, there are still individuals who would rate their level of knowledge lower than a 3 out of 5. When a participant responds with a 2 or a 3, it is usually accompanied with "I would like to know more", or "I wish I knew more." There was one older participant who defined his/her level of knowledge and concern at a 5. Yet when answering the true/false questions about their online and offline privacy knowledge, this individual answered all nine incorrectly. He/she believes that they know more about technology and what companies can know about them. However, when showing their actual knowledge, it is obvious that they do not know as much as they perceive they know. There was a different older individual who rated a 5 both on knowledge and concern, and got three of nine questions incorrect. Meanwhile, younger individuals who rated themselves at a 2 or 3, answered 1 or none incorrectly. There is a misconception of what the participants know about technology, and they are unaware of these misconceptions.

DISCUSSION

This study revealed several common themes that help shed light on the varying perceptions of privacy among participants. Among study participants, younger adults accept that their personal data will be collected by companies; however, they do not want their information to be abused or mishandled. When asked if participants knew what companies did with their data, one participant responded with "no, but I would like it to not be used other than for what they need it for". Older individuals actively avoid companies or organizations that seek too much information, where younger adults seem to hope for the best and give their information. One participant stated, "If it's something I am concerned with [for] a company, then, I try not to do business, or I try to find the privacy thing that says no don't send me all this stuff." Through this study, older individuals will actively go out of their way to protect their privacy, while younger individuals accept that companies will sell some information.

The participants displayed varying levels of precautionary actions. When asked if they refused to provide information to an organization, the way in which participants responded shows the underlying perspective of privacy. When comparing the two responses, most young adults stated, "I'm sure I have," where older adults stated, "Definitely! Oh absolutely." It appears that older individuals would actively refuse to provide information when stating "definitely," where younger individuals do not normally decline that information, but assume they must have done so at some point. There seems to be a willingness that younger individuals have towards divulging information that older individuals do not have. Perhaps younger individuals are more accustomed to others having and collecting their data, as they have grown with technology.

The participants displayed a consistent misunderstanding of technology. This shows that regardless of age, everyone has some misconceptions and misunderstanding about technology and online privacy rights. Many believe that they

have more privacy than they actually do, but, at the same time, they believe that companies infringe on those rights regardless of regulations.

Finally, most participants realized they lack knowledge related to privacy rights. However, all participants rated themselves higher in knowledge than their question scores measured. This result suggests much more privacy awareness and training are needed.

LIMITATIONS

This study had limitations, including a time constraint, convenience sample, and low number of participants. The study was conducted as part of 8-week intensive scholarly research program. Due to the time constraint, a convenience sample was utilized. Convenience samples are vulnerable to selection bias, sampling error, and are not representative of a larger population. The participation numbers for the focus groups were not adequate to draw substantial conclusions. Due to this, the researcher changed to one-on-one interviews. This proved to be far more effective, allowing for more immediate interviews.

CONCLUSION

Individuals, regardless of age, want online privacy. Many of the participants in this study want privacy but do nothing to obtain it. However, there does appear to be a more pessimistic view point from older individuals. Younger individuals have different privacy expectations than older individuals. When looking at the age difference between generations in this study, older participants also seem to either know about as much about technology as younger individuals or simply disregard technology. Similarly, there are three classifications for students that can also be applied to older individuals. Many older individuals either immerse themselves in technology or use it sparingly while another group disregard it entirely, perhaps not specifically naïve or meh individuals as described by Marreiros et al., (2015), but the approach is similar. Many older individuals in this study echoed the same: "It is necessary in today's society to use Facebook," and it comes with risk. Older individuals equate online activities to driving a car. You run the risk of a car accident, but you drive regardless. You need to purchase an item from the internet, so you take the risk regardless of credit card theft. Technology will never stop advancing and the consumers must be aware what companies are doing with their information. Based on this study, individuals must re-evaluate their preconceived notions of technology to better understand how to protect themselves.

REFERENCES

Byrne, Z. S., Dvorak, K. J., Peters, J. M., Ray, I. Howe, A. & Sanchez, D. (2016), From the user's perspective: Perceptions of risk relative to benefit associated with using the Internet. *Computers in Human Behavior, 59*, 456-468.

Diane, G., & Lily R., J. (2015). Social Networking Privacy—Who's Stalking You?. *Future Internet, 7*(1), 67-93.

Doughty, H. A. (2014). Surveillance, Big Data Analytics and the Death of Privacy. *College Quarterly*, *17*(3), Retrieved from https://eric.ed.gov/?id=EJ1049869

Halperin, R., & Dror, Y. (2016). Information privacy and the digital generation gap: An exploratory study. *Journal of Information Privacy & Security*, *12*(4), 166-180.

Hoofnagle, C., King, J., Li, S., & Turow, J. (2010). *How different are young adults from older adults when it comes to information privacy attitudes & policies*. http://dx.doi.org/10.2139/ssrn.1589864

Kirk, D. (2014). Identifying Identity Theft. *Journal of Criminal Law, 78*(6), 448-450.

Krebs, B. (2014). *Spam nation: the inside story of organized cybercrime--from global epidemic to your front door.* Naperville, IL: Sourcebooks.

Mamonov, S., & Benbunan-Fich, R. (2015). *An empirical investigation of privacy breach perceptions among smartphone application users. Comput. Hum. Behav. 49, C (August 2015), 427-436. DOI=http://dx.doi.org/10.1016/j.chb.2015.03.019*

Marreiros, H., Gomer, R., Vlassopoulos, M., Tonin, M., & Schraefel, M. C. (2015). Scared or naïve? An exploratory study on users perceptions of online privacy disclosures IADIS International Journal on https://eprints.soton.ac.uk/id/eprint/399150, 13 (2), 1-16.

Phoenix Strategic Perspectives Incorporated. (2013). Survey of Canadians on privacy-related issues. Ottawa: Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/media/3323/por_2013_01_e.pdf

Ritvo, E (2012, May 24). Psycology Today. Retrieved from Facebook and your brain: https://www.psychologytoday.com/blog/vitality/201205/facebook-and-your-brain

Salazar, M., & Woodard, B. (2017). With Great Data, Comes Great Responsibilty. *Issues in Information Systems Journal, 18*(1), 191-201.

Zurbriggen, E. L., Ben Hagai, E., & Leon, G. (2016). Negotiating privacy and intimacy on social media: Review and recommendation T*ranslational Issues in Psychological Science, 2*(3), 248-260.

APPENDIX A

Questions utilized for the study pulled from *A Survey of Canadians on privacy-related issues* Phoenix Strategic Perspectives (2013).

Instructions: Using a scale from 1-5, 1 being the lowest and 5 being the highest, rate each of the questions.

- How would you rate your level of knowledge of privacy rights?
- How would you rate your level of concern over personal privacy?
- What do you think the likelihood is of someone using your saved online credit card information (i.e., Amazon) to make unauthorized purchases?
- What do you think the likelihood is of someone accessing the personal information on your computer or mobile device without your permission?

Instructions: For the following questions, respond if you are concerned with any of the following possibilities?

- Wearable technology that collect personal information from the wearer
- Public institutions or alumni associations selling personal information
- Security of university school systems or email accounts
- Security of your social media accounts
- Do you have a social media account?
- Do you have any photos uploaded to the account?
- How many of those were uploaded by someone else? Say by friends or family?
- Of those how many got your permission?
- Should sites ask for permission?
- Do you believe that email puts you in more risk than a social media account?
- Do you feel confident that you have enough information to know how new technologies will affect your personal privacy?
- Do you feel that you have less protection of your personal information in your daily life that you did 5 years ago?
- Do you feel confident that when you share your personal information with an organization, you understand how it will be used?
- Have you ever been negatively affected as a result of an organization misusing, sharing or losing your personal information?
- In your opinion, do you believe that private social media accounts are really private?

- Do you use a password lock on your phone?
- Have you ever refused to provide an organization with your personal information?

APPENDIX B

Questions utilized in this study, pulled from *How different are young adults from older adults when it comes to information privacy attitudes & policies* Hoofnagle et al. (2010).

Instructions: Below are a series of true/ false statements. Please indicate whether they are true or false.

- If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission.
- If a website has a privacy policy, it means that the site cannot give your address and purchase history to the government.
- If a website has a privacy policy, it means that the website must delete information it has about you, such as name and address, if you request them to do so.
- If a website violates its privacy policy, it means that you have the right to sue the website for violating it.
- If a company wants to follow your internet use across multiple sites on the internet, it must first obtain your permission.
- Offline Questions Answer
- When you subscribe to a newspaper or magazine by mail or phone, the publisher is not allowed to sell your address and phone number to other companies without your permission.
- When you order a pizza by phone for home delivery, the pizza company is not allowed to sell your address and phone number to other companies without your permission.
- When you enter a sweepstakes contest, the sweepstakes company is not allowed to sell your address or phone number to other companies without your permission.
- When you give your phone number to a store cashier, the store is not allowed to sell your address or phone number to other companies without your permission.
- After the conclusion of the interview, I reiterate the initial questions to see if their response would change.
- How would you rate your level of knowledge of privacy rights?
- How would you rate your level of concern over personal privacy?

*** All answers for the questions are false**.

APPENDIX C

The mean of the numerical results from the interviews. Questions 1-4 pulled from Phoenix Strategic Perspectives (2013).

	Younger	Middle-age	Older
	(18-25)	(26-45)	(46-63)
How would you rate your level of knowledge over privacy rights?	2.25	3.25	3.25
How would you rate your level of concern over personal privacy?	3.125	3.25	4.5
What do you think the likelihood is of someone using your saved online credit card information (i.e., Amazon) to make unauthorized purchases?	2	3.375	3.5
What do you think the likelihood is of someone accessing the personal information on your computer or mobile device without your permission?	2.5	2.5	2.5