https://doi.org/10.48009/1_iis_2017_191-201

Issues in Information Systems
Volume 18, Issue 1, pp. 191-201, 2017

WITH GREAT DATA, COMES GREAT RESPONSIBILITY: UNIVERSITY STUDENTS' PERCEPTIONS ON DATA PRIVACY

Maria Salazar, Southern Illinois University Carbondale, mariasalazar93@siu.edu
Belle Woodward, Southern Illinois University Carbondale, bellew@siu.edu

Abstract

The purpose of this study is to add to the current research concerning the differing perceptions of data privacy among various groups of people, in this case college students who attend a large, Midwestern university. This study is conducted to better understand how university students view their privacy rights related to their use of technology. Qualitative data were collected through focus group discussions with 18 students from different disciplines throughout the university. The focus group results suggest that university students have a high level of concern over their data privacy, but lack the knowledge to protect themselves. Additionally, the Millennials, primarily university-aged students, were the first group to begin using technology and social media on a regular basis which leads to a demonstration of carelessness regarding what personal information they post online.

Keywords: Data Privacy, Information Technology(IT), Students, University, Perceptions, Data, Privacy

INTRODUCTION

In today's world, it's difficult to find an aspect of life that can't be integrated with technology. Long gone are the days of notepads and checkbooks; in their place iPads and debit cards are being used widely. With this ever-growing integration of technology into our everyday lives comes the opportunity for personalization leading to an ever-increasing amount of personal data being shared online and with our devices. This excess data sharing has raised concerns about how private our personal data may actually be.

Living in an environment where technology is constantly used to complete assignments, check emails and stay connected through social media, college students are among the most prominent demographics that should consider data privacy as a cause for concern. The article posted by Marketplace entitled "Do You Know What Your College is Doing With Your Data?" says it best when they say, "By the time most college freshman step on campus, it's a good bet Facebook knows who their friends are, Amazon knows what they buy, Netflix knows what they watch and Google knows…well, pretty much everything they do online" (Newman, 2014). Jay Stanley, a senior policy analyst with the American Civil Liberties Union's Speech and Privacy Project, says "College students are of an age where they haven't started their careers yet; they're getting ready to go out in the world and be judged." He continues by explaining that students need privacy as they begin exploring new personal identities in college because, sometimes, this exploration is not something you want to stick with you forever (Tablante, 2013).

When discussing data privacy in a university setting, you will often hear students say they "have nothing to hide" regarding their privacy and use of information online. However, when it comes to data privacy, it isn't a matter of whether one should care, it's a matter of what personal rights regarding privacy a person should be entitled to as well as how simple a malicious attack on their personal data could be.

Many people in the technology field are familiar with the cyber-attack on Wired Magazine's Mat Honan. Using security holes found in Amazon and Apple accounts, hackers were able to gain access first to Mat's Amazon account and use that information to access his Apple account. Once both accounts were available to the hackers, they utilized his private information to delete his Google account, hijack is Apple ID, take over his Twitter, delete backups made of his iPad and iPhone, wipe his iOS devices, and completely erase his MacBook which contained all the pictures from the first year of his child's life (Smith, 2012).

If even an informed techie working for a major technology magazine such as Wired can be undereducated and defenseless against an attack so simple yet so malevolent as this, college students with such a care-free attitude regarding their data privacy are even more susceptible. David Jacobs, the consumer protection counsel for the Electronic Privacy Information Center, says, "The importance of maintaining online privacy is the idea that some aspects of your life or behavior should be free from surveillance" (Tablante, 2013). Understanding the current perceptions university students have can help gauge what should be done to help educate them on their rights and how to better defend themselves against increasingly invasive technology.

LITERATURE REVIEW

Previous Studies on Perceptions of Data Privacy

In the initial study of Canadians by Phoenix Strategic Perspectives Incorporated regarding privacy related issues, a majority (63%) rates their knowledge of privacy laws as low to neutral on a 7-point scale. Many of them are aware that their ability to protect their information is shrinking. When asked, 7 out of 10 people believe they have less protection in their daily lives than they did 10 years ago and a majority believe they do not have enough information to know how new technologies will affect their personal privacy. Despite a concern by the majority, only 21 percent have ever actively sought out information about privacy rights. Many Canadians, however, are reluctant to share their information and almost all would like to be notified if their personal information were to be compromised (Phoenix Strategic Perspectives Inc., 2013).

In a German study based on the aforementioned Canadian study, a majority of Germans expressed high levels of concern over their personal privacy but lacked knowledge about what rights they may have. In this study, people with a university degree rated their "level of knowledge of privacy rights" higher than those who did not have a university degree and were overall less concerned. There was distrust with companies and government regarding data privacy, however, most people tended to trust small companies over larger ones. There was a common conception that the government wasn't able to protect itself, let alone the information of citizens. Similar to the Canadian study, many Germans are concerned about the privacy of their data but do not take action to seriously protect it (Brownlee, Ewald, Geiger, Jahn, Jaser & Knauer, 2015).

How College Students Currently View Online Privacy

According to a section of a 2015 study conducted by the Media Insight Project on how Millennials get their news entitled Digital Lives of Millennials, the first generation of digital natives were born in 1980 and entered high school as the internet became a public forum. Of this group, half, those aged 26 and under, entered high school using social media. For the majority of this generation, this digital revolution has become the norm, and consequentially it is believed this integration of technology into their everyday lives has led to a rather lax attitude towards data privacy. In fact, when asked, 46 percent of the participants were cited as having "little worry" about their privacy online (MIP, 2015, "How Millennials Get News", sect. 4).

This nonchalant attitude of Millennials isn't anything new, however. In 2011, when the Online Advertising Industry unveiled a do-not-track icon for web browsers, college students were undecided as to whether the privacy feature was really necessary. This issue seems to be primarily related to college-aged students' lack of awareness and education on the matter. In an article about the do-not-track icon, put out by USA Today, two college sophomores from different schools were quoted as being "unaware that an opt-out existed" and "unaware of tracking features on the Web browser" (Levine, 2011). In another article by USA Today titled "How college students can maintain online privacy", a junior at the University of Maryland believes most people aren't aware of the personal information they are sharing from their web browser. The bigger issue here is that people are being tracked in ways they either aren't aware of or don't understand (Tablante, 2013).

However, whether the concern for protecting their data is high or low, most university students were in agreement about their concerns regarding data privacy. In the study published by the American Press Institute, 38 percent of all participants interviewed cited their number one concern being that someone would steal their identity or financial

information. A second concern that seemed to be a trend among college students, with nearly 40 percent having considered it, was the worry of potential employers or schools forming unfair impressions of them based on their online footprint (MIP, 2015, "How Millennials Get News", sect. 4). The latter is one situation that David Jacobs, of the Electric Privacy Information Center, believes college students should be concerned about and advises them to be cautious with the information they disclose online (Tablante, 2013).

Schools, Universities and Affiliates Selling Student Data

In a technology article published by Forbes, "Your Kid's School May Have The Right To Sell Student Data", 6 in 10 parents said they had heard little or nothing about schools allowing private companies to store personal data about their children (Shapiro, 2014). If schools with students young enough to need parental consent to share personal data are already allowing private companies to store it, imagine the situation in an institution whose students are primarily legal, consenting adults.

College campuses collect all kinds of data other than just a student's grades and transcripts. Students give their data every time they check out a book from the library, log on to the campus Wi-Fi network, swipe an ID card or key FOB to enter a dorm, buy lunch in the dining hall, post an assignment on a class discussion board and almost throughout every other part of their day. Typically, colleges don't hand out data-use agreements and privacy policies to their students for this data either, the way companies like Facebook and Google might do. Due to these blurred lines, the bigger question is, who really owns this data, the students or the colleges (Newman, 2014)?

Many colleges try to use this data for the betterment of their student community. From this information, they try to predict student behavior and craft interventions for students at risk of dropping out as well as help direct students into classes and majors in which they are most likely to succeed. However, with great data comes great responsibility. Universities are already juicy targets for hackers owed to student records, including social security numbers as well as credit card and financial information of the students and their family members, being stored in networked computers or personal devices. Aside from potential hacks, there are also loopholes to be found allowing colleges to indirectly sell student data to companies (Newman, 2014). An extreme example of this could be seen when the alumni association at the University of Iowa sold student data to Bank of America for profit. The agreement was that Bank of America would have guaranteed access to home addresses, phone numbers, and e-mail addresses of University of Iowa Students and their parents. The university would provide the alumni association with student information as well as parent and other alumni information from databases related to sporting events, and the alumni association would then sell it to Bank of America. Although unethical, the alumni association is seen as a private entity, whereas the university is not, and was legally able to enter into the deal (Marco, 2007).

The University of Iowa example, however, is not the only one of its kind. Such a roundabout way of buying data is an approach used by Bank of America and multiple other credit card companies to obtain data from many U.S. schools (Marco, 2007). The CEO of the education technology company, Common Sense Media, believes "schools should be completely off limits when it comes to collecting personal information of students for marketing purposes." In agreement with this, 85 percent of adults believe the government could do more to protect student data (Shapiro, 2014). A freshman at Oberlin College said if they are going to feel uncomfortable about giving out data, it shouldn't be to a university to which they pay thousands of dollars in tuition, an organization they feel a personal connection with (Newman, 2014).

Wearable Technology Companies Selling Personal Data

In this day and age, wearable technologies such as smart watches and fitness trackers have become a staple in society. The wearable wrist-band devices can track many things including weight, mile splits, steps taken per day, sleep quality, sexual activity, calories burned and even your GPS location. While the purpose of these trackers is to monitor health, we are able to send this information to various websites and apps. If users aren't careful, this personal data could end up in the hands of corporations that could use it to market other products and services; make decisions about eligibility for credit, employment, or insurance; and even share this data with other companies (Liebelson, 2014).

While many of these wearable technology companies claim they don't sell your data, there are often some loopholes to be found. With FitBit, device users have the option to automatically send their fitness data to the FitBit website, where you are encouraged to submit other medical information such as blood pressure and glucose levels. However, if you read their privacy policy close enough, you will find that "FitBit may make certain personal information available to strategic partners that work with FitBit to provide services to you". Nike's privacy policy states that the company may collect a host of personal data, but will not share it with "outside" advertisers. However, the companies that fall underneath Nike's corporate umbrella are fair game. Garmin requires that users consent before they will sell any of your personal information. The company PolarFlow is the only company, in an article put out by Mother Jones, which has a privacy policy specifically stating it will not sell personally identifiable data for advertising. However, every day we constantly see people walking around with FitBits, Nike + Fuel Bands and Garmin Vivofits. How often have you heard of the Polar Loop Band? As for the companies that may not be profiting from your personal data, Jeffery Chester, the executive director for the Center for Digital Democracy says if companies aren't selling your data now, it's only because they haven't developed a business model to do so yet (Liebelson, 2014).

Since Mother Jones put out that article in 2014, FitBit has started profiting from users' health data by selling it as a company health initiative where employers can track their workers' health. Companies that have participated in this FitBit tracking software have seen reduced group insurance pricing as a result of healthier employees (Smith, 2014). However, not all companies are entering this market in the same positive way as FitBit. A San Francisco startup called Big Health licenses its insomnia treatment app Sleepio to more than a dozen employers. Sleepio is effectively a Trojan horse which employers can use to tackle mental health issues in their workforce without raising privacy hackles (Olson, 2016).

Nevertheless, your employers monitoring your health is probably a less-likely privacy concern than the use of third party fitness apps users may be sending their personal data to. Once a user's data are subject to the privacy policies of the app, not just of their wearable device or smartphone, they don't have much protection against the misuse of the data (Liebelson, 2014).

How College Students View Social Media Privacy

Younger Millennials, including college-aged students, are more likely to use a mix of social networks with the average 18-to-21-year-old using 3.7 social networks out of seven platforms (MIP, 2015, "How Millennials Get News", sect. 5). In a study conducted at Pace University, it was found that about 90 percent of students at academic institutions are on social media sites daily (Lawler & Molluzzo, 2009).

In a study published in the Journal of Computer-Mediated Communication, out of 1,710 students included in the population, 33.2% had private profiles on Facebook; of these, 93.1% had private profiles that were not searchable at all. This study also found the more frequently a user changed their profile, the more likely they were to adopt a private profile. Additionally, they were more likely to have a private profile if their friends and roommates also had private profiles (Lewis, Kaufman & Christakis, 2008).

On Facebook, it was found that nearly everyone stores their name and gender; many store the names of friends, photos and age; and a surprisingly high number, around 16-17%, store highly personal data such as their telephone number and address (Lawler & Molluzzo, 2009). Facebook, in particular, requires users to identify themselves authentically. Although we know this doesn't always happen, it is written into their Terms of Use that users may not "impersonate any person or entity, or falsely state or otherwise misrepresent yourself, your age or your affiliation with any person or entity" (Lewis, Kaufman & Christakis, 2008).

With such a high number of college students putting personal data on social media and utilizing privacy settings, not many of them seem very concerned about the privacy of their data. In general, the millennial generation is not highly concerned about privacy, with their biggest changes being related to paying more attention to privacy settings than before and removing embarrassing or immature content (MIP, 2015, "How Millennials Get News", sect. 5). In the Pace University study, barely half of the students indicated issues pertaining to security and privacy on social media to be problematic or risky (Lawler & Molluzzo, 2009). The study published by the Journal of Computer-Mediated Communication cites instances when students' social media profiles prevented them from getting a job or resulted in

campus police crashing a party, and yet the common conception seems to be privacy isn't a matter for concern (Lewis, Kaufman & Christakis, 2008).

This issue of lack of concern seems to stem from a lack of education on the subject. The concern of the authors of the Pace University study was students of the Millennial generation lack the knowledge of the fact, or the impact of the fact, that characteristics of social networking are inherently public on the Web (Lawler & Molluzzo, 2009). Studies have collected profile information on Facebook through the use of web crawlers and surveys; this information shows that users reveal a lot of information about themselves and don't seem very aware of who is able to see their profile. When on a social network of millions of people, it's not realistic to trust them all. Something embarrassing attached to the public profile of a friend could potentially be associated with your account. Even the social networking sites themselves are recording all interactions and retaining them for use in data mining. A digital message never really goes away; it stays in the system for an undefined and unknown period of time. However, in a study submitted to the Americas Conference on Information Systems, it was found that a mean of 4.97 said that they "trust that the social network site will not use my personal information for any other purpose" (Dwyer, Hiltz & Passerini, 2007).

RESEARCH METHODOLOGY

A qualitative research design was used for the purpose of this study. To have the best understanding of the perceptions university students have regarding data privacy, focus group interviews were conducted in an effort to capture direct quotes from the participants' personal experiences and ideas. Focus group interviews allowed the researcher to ask open-ended questions and gather as much information as possible from the subjects. The group setting made discussion between the subjects easier and allowed a flow of opinions that each person could elaborate on. This led to the collection of copious data and information. The researcher also used purposeful sampling, selecting one group of Information Systems Technologies students, and two others that were not technology focused, Agriculture and Law, to better understand how education on technology would affect students' difference in perceptions.

For this research study, the researcher conducted three focus group interviews and the sample population are shown in Table 1. Groups I and A each had seven subjects and Group L had four. The focus group facilitator identified herself as an undergraduate student working on an Honors Program thesis research study that pertains to data privacy perceptions. Written informed consent was obtained from subjects. Two focus groups were audio recorded to be analyzed and transcribed at a later time. The third group, due to time constraints, discussed the questions on their own time and provided the researcher with written responses to the research questions. The groups were all asked the same twelve questions, as follow.

- 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?
- Are you concerned about 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 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?

The focus group facilitator read the questions and allowed time for each participant to answer. Not every participant had an answer for every question. Some of them chose to agree with others who responded, or did not provide an answer at all. Each participant was assigned a number in an effort to keep his or her identity anonymous. Group A included participant A1 through A7, Group I included participant I1 through I7, and Group L included participant L1 through L4. The groups were assigned letters instead of numbers so that the college of the participants could still be identified for analyzing the responses; the participants were assigned a number 1-x that correlated with their group letter.

Using purposeful, homogenous and convenient sampling worked out well for this study. The goal was to focus on the particular perceptions university students have regarding their data privacy. Due to time constraints and lack of resources, a convenience sample was used. Information Systems Technologies majors were chosen as the technology savvy participants due to the researchers' association with the major. Agriculture and Law students were also chosen because they were readily available to the researchers through personal connections.

Table 1. Demographics

Group	College	No.	Gender	Age	Major
Group A	College of Agriculture	7	M	22	Crop, Soil & Environmental Science
			M	22	Agriculture Systems Technology
			M	20	Crop, Soil & Environmental Science
			M	22	Forestry
			M	22	Forestry
			M	21	Crop, Soil & Environmental Science
			M	28	Forestry
Group I	College of Applied Sciences & Arts	7	M	21	Information Systems & Applied Technologies
			M	22	
			M	23	Information Systems & Applied Technologies
			M	27	
			M	24	Information Systems Technologies
			M	21	Information Systems Technologies
			M	21	Information Systems Technologies
					Information Systems Technologies
					Information Systems Technologies
Group L	School of Law	4	F	25	2nd Year Law
			F	24	2nd Year Law
			F	23	2nd Year Law
			F	36	Doctor of Law

RESULTS

Analyzing focus group transcriptions revealed various themes. Themes derived included:

- low level of knowledge of privacy rights
- personal information on certain devices is more at risk than others
- concern with university related privacy rights
- diminished protection due to lack of confidence in new technology
- unsure of how companies use data but take precautions

Low Level of Knowledge of Privacy Rights

Focus group participants were students studying Information Systems Technologies, Agriculture and Law but all agreed they had a medium to low level of knowledge regarding privacy rights. Most of the participants said they either didn't know much about it or didn't know as much as they probably should. Other participants generally agreed with this reasoning.

The group of students studying Agriculture generally agreed they didn't have much knowledge about privacy rights. Two of the seven participants of this group confirmed their lack of knowledge by citing stolen identities or credit card information. The Information Systems Technology group believed that while they were aware of some aspects and policies, they should be more educated given their area of study. The Law students took a legal standpoint stating they were "knowledgeable about the rights the Constitution provides us but not state law or otherwise".

Despite this low level of knowledge, there was a clear split between whether or not students were concerned about their own personal privacy. Seven out of the 18 participants gave a response rating their level of concern as high. Many of the other responses aligned with being "not that concerned" due to a lack of knowledge or just putting it out of their mind. Notwithstanding these different levels of concern, all 18 participants at least take precautions to protect the personal information encompassed in their cell phones by using some type of lock or passcode.

Personal Information on Certain Devices is more at Risk than Others

All participants from the three groups rated the likelihood of someone accessing their personal information on their computer or cell phone without their permission between medium and high. Different degrees of personal information being accessed were mentioned, starting with ad-tracking on a Google search and moving all the way up to drive-by attacks using devices that incorporate radio-frequency identification (RFID) technology to access devices within a five foot radius; these devices, used to steal information, have the capability to do so within 30 seconds.

Although most people considered the likelihood of someone accessing their personal devices without authorization to be on the higher side of the scale, the participants had more mixed views and less concern over the idea of someone accessing your saved credit card information on shopping sites like Amazon. About half of the participants believed the likelihood of this to be high and saw it as a common problem. The other half, however, considered the likelihood higher based on certain situations. A couple of members of the Agriculture group said they try to keep their online, saved credit card information to a minimum and credit this to their belief that the likelihood for them, personally, isn't very high. The Information Systems Technology group had a view similar to this but in a broader sense. They viewed the likelihood of online credit card information being stolen as being closely related to a person's level of knowledge on how to protect themselves online.

All of the participants agreed they weren't very concerned about wearable devices, particularly health tracking devices, which collect personal information. This was predominantly due to the type of information these devices collect and the perception that health information, such as step count or calories burned, is not as intimate or private as something like financial information or social security numbers. The concern was higher when it came to wearable devices such as smart watches that are synced up with a cell phone, due to the fact that the ability to access personal information on the watch meant a direct connection to the information that a person's cellular device may contain.

Concern with University Related Privacy Rights

When questioned about their concerns related to universities or alumni associations selling personal information of students, every single participant agreed that it was a serious cause for concern. A surprisingly large number of participants were even cited as saying they "didn't know it was even a thing". The primary argument around this perception was if data belongs to you, no one else—including universities or alumni associations you pay for—should have the right to sell it to any other person or entity for any reason. One student in the Agriculture group even claimed that the university or association asking his approval to sell it could make the situation tolerable, but not favorable.

Every participant in the focus group research had a serious cause for concern regarding the security of university schooling systems, primarily for email accounts. For this question, every participant touched on some aspect of the incredible amount of spam or technical issues they receive as a result of having an email account registered to the

domain of a large Midwestern university. Although most of the concerns were represented with a level of annoyance with the excess email spam, one of the Information Systems Technology members brought up a very valid security concern. This person explained that it was alarming given the amount of effort these hackers put into recreate official university emails and addresses, whereby it has become extremely difficult to tell the fake from the real when spammers use accounts ending with the university ".edu" domain.

Diminished Protection Due to Lack of Confidence in New Technology

All eighteen participants in this study were in agreement that they had less protection over their personal information than they did five years ago. Many cited the integration of technology into our everyday lives as the primary reason for this decrease in security. When you are constantly wired in with smart phones, social media, and email accounts, there's more room for carelessness to creep in. These participants claimed many times, they enter personal information into their devices and accounts without even thinking twice.

With technology being more closely incorporated into our everyday lives than it was five years ago, the pace of development of new technologies has increased immensely. All eighteen participants agreed once again they were not confident they had enough information to know how new technology would affect their personal privacy. One member of the Information Systems Technologies group explained that one couldn't because technology is constantly evolving, stating the same processing power we used to complete the Mars Mission is now the processing power we use in our smart phones on a daily basis. Almost all of the participants, however, were conscious and accepting of the fact that technology would constantly change and they wouldn't know how this flux might affect them and their personal privacy.

Unsure of How Companies Use Data but take Precautions

All participants came to a common consensus that upon sharing personal information with an organization, they lacked the confidence to understand how their data would be used. Participants in two of the three groups cited this as a direct correlation to the fact that they completely skip over user agreements. A member of the Agriculture group admitted they might not have a full understanding of the terms and conditions outlined for them. The Information Systems Technology group also admitted they often skip through the agreements just to get it over with and continue the process they were trying to complete. They also joked saying organizations could intentionally make user agreements longer and in smaller print in order for people to ignore them and agree to the terms therein without reading.

Although all the participants were unsure of how companies might use their data, a majority of them claimed to have personally never been negatively affected by an organization misusing, sharing or losing their personal information; however, they knew someone who had. In order to further protect oneself from being a victim of this exploitation in the future, every participant stated they had, at some point, refused to provide an organization with their personal information. However, if they did provide personal information, they were most likely to provide an email address over anything else. However, even that has been refused when it comes to things like stores asking for an email address for coupons, if it's not something they want to receive.

DISCUSSION

The idea that university students seem to have a high level of concern about their personal privacy but lack the knowledge to protect it aligns with the Canadian and German studies done on data privacy. This idea is also the same in that a majority of the students in this study perceive they have less protection for their information than they had in previous years and they lack the knowledge of how new technologies affect their own personal privacy.

This idea also corroborates literature regarding perceptions college students have concerning data privacy. Almost all the participants in this study fall into the Millennial category, outlined in the study "How Millennials Get News", given they entered high school using either the Internet or social media. In this study, it is stated that the early integration of technology into the lives of this age group has caused them to become immune to issues concerned with the privacy of their data (MIP, 2015, "How Millennials Get News", sect. 4). This is evident from the fact that

participants in this study claimed being careless and they did not think twice about the personal information they enter online or into their devices. This is especially eye opening because all eighteen participants agreed they were not confident about how organizations would use their personal data.

Some participants in this study cited ad tracking as a means someone would use to covertly access your personal information on your devices. This was an expected response because the literature on college students' data privacy perceptions includes an article by USA Today where university students were quoted as saying they were "unaware that an opt-out existed" and "unaware of tracking features on the Web browser" (Levine, 2011).

Although the student data transaction between the University of Iowa and Bank of America—which has been summarized in the literature—may be a more extreme example of this concept; universities selling or providing student information to businesses for gain is not a new concept. However, based on the bewildered responses of the participants of this study, universities seem to be keeping these unethical arrangements well under wraps. Following the mantra of out of sight, out of mind, if colleges keep this information transfer secret, the students may never realize their data is being accessed.

One aspect which was not a common conception mentioned in the findings was the outlook on social media privacy among the participants. When asked if they believed private social media accounts were really private, the answers varied. Some of the participants believed nothing was private or hidden for anyone, while others believed certain aspects of a social media page can be private but others cannot be. A few other participants mentioned that a private social media account might be private to other users, but nothing is going to be private from the company. A section of students in this study also had social media accounts they did not post on or did not have social media accounts at all. This was surprisingly lower than the average 3.7 social media networks that 18-to-21-year-olds were cited to be using in the article "How Millenials get News". However, the perceptions the participants had concerning social media privacy coincide with the statement students lack the knowledge of the fact—or the impact of the fact—that characteristics of social networking are inherently public on the Web (Lawler & Molluzzo, 2009).

LIMITATIONS

As this study was conducted under strict time constraints, a better level of understanding could be gained by conducting a larger number of focus groups from a greater range of colleges throughout the university. Using a more equally balanced population of students from different colleges as well as gender could also have a different effect on the outcome of the study. The questions in this study were kept more general in order to incite a better discussion among participants of each group. However, a better comparison among responses could be made if questions were made to focus on more specific topics.

CONCLUSION

In order for college students to better protect themselves against damaging or unauthorized uses of their personal information, we need to understand how they perceive their own data privacy rights. With an increasing integration of technology into everyday life, remarkably so in the lives of university students, there comes a responsibility to secure the personal information that is shared. College students tend to present particularly more lenient attitudes toward online and personal privacy and present a lack of knowledge about how to secure their data; an evaluation of their perceptions of data privacy could prove to be beneficial in implementing a way to raise awareness about this matter and motivate university students to take responsibility and protect their personal information

REFERENCES

Dwyer, C., Hiltz, S. R., & Passerini, K., (2007). T*rust and privacy concern within social networking sites: A comparison of Facebook and MySpace*. Retrieved March 12, 2017, from AMCIS 2007 Proceedings: http://aisel.aisnet.org/amcis2007/339

Lawler, J. P. & Molluzzo, J. C. (2009). *A study of the perceptions of students on privacy and security on social networking sites (SNS) on the Internet*. Retrieved November 3, 2016, from EDSIG Proceedings: http://www.proc.conisar.org/2009/3732/CONISAR.2009.Lawler.pdf

Levine, S. (2011). S*tudents still struggling with Internet privacy.* Retrieved December 4, 2016, from *USA TODAY:* http://college.usatoday.com/2011/08/31/students-still-struggling-with-internet-privacy/

Lewis, K., Kaufman, J. and Christakis, N. (2008). T*he taste for privacy: An analysis of college student privacy settings in an online social network*. *Journal of Computer-Mediated Communication, 14: 79–100*. doi:10.1111/j.1083-6101.2008.01432.x

Liebelson, D. (2014). *Are Fitbit, Nike, and Garmin planning to sell your personal fitness data?.* Retrieved March 20, 2017, from Mother Jones: http://www.motherjones.com/politics/2014/01/are-fitbit-nike-and-garmin-selling-your-personal-fitness-data

Marco, M. (2007). *Alumni associations and public universities profit by selling student data to Bank of America.* Retrieved December 11, 2016, from *Consumerist:* https://consumerist.com/2007/09/24/alumni-associations-and-public-universities-profit-by-selling-student-data-to-bank-of-america/

MIP. (2015). *How Millennials get news*.. Retrieved December 10, 2016, from American Press Institute: https://www.americanpressinstitute.org/publications/reports/survey-research/digital-lives-of-millennials/

Newman, J. (2014). *Do you know what your college is doing with your data?*. Retrieved February 18, 2017, from *Marketplace:* https://www.marketplace.org/2014/09/25/education/learning-curve/do-you-know-what-your-college-doing-your-data

Olsen, P. (2016). *Fitbit's game plan for making your company healthy*.. Retrieved February 12, 2017, from Forbes: https://www.forbes.com/sites/parmyolson/2016/01/08/fitbit-wearables-corporate-wellness/#33c57afd5ff6

Phoenix Strategic Perspectives Incorporated. (2013). Survey of Canadians on privacy-related issues.

Shapiro, J. (2014). *Your kid's school may have the right to sell student data.* Retrieved January 12, 2017, from Forbes: https://www.forbes.com/sites/jordanshapiro/2014/01/24/your-kids-school-may-have-the-right-to-sell-student-data/#1dfad5ee68b5

Smith IV, J. (2014). *Fitbit is now officially profiting from users' health data.* Retrieved March 7, 2017, from Observer: http://observer.com/2014/04/fitbit-is-now-officially-profiting-from-users-health-data/

Smith, W. (2012). *How to protect yourself from Amazon's and Apple's gaping security holes.* Retrieved from Adam Savage's Tested*:* http://www.tested.com/tech/web/142106-how-to-protect-yourself-from-amazons-and-apples-gaping-security-holes/ - mat from wired security hack from amazon and apple

Tablante, M. (2013). *How college students can maintain online privacy.*. Retrieved December 12, 2017, from USA TODAY: https://www.usatoday.com/story/tech/personal/2013/04/23/college-students-online-privacy-tips/2107313/