

## **Privacy Education Effectiveness: Does It Matter?**

Matthew Heinrich and Natalie Gerhart

**Recommended Citation:** Heinrich, M., & Gerhart, N. (2023). Privacy Education Effectiveness: Does It Matter? *Journal of Information Systems Education*, 34(1), 49-69.

**Article Link:** <https://jise.org/Volume34/n1/JISE2023v34n1pp49-69.html>

Received: January 6, 2022  
Revised: March 18, 2022  
Accepted: June 21, 2022  
Published: March 15, 2023

Find archived papers, submission instructions, terms of use, and much more at the JISE website:  
<https://jise.org>

ISSN: 2574-3872 (Online) 1055-3096 (Print)

---

# Privacy Education Effectiveness: Does It Matter?

**Matthew Heinrich**

Department of Mathematics, Analytics, and Technology  
Rockhurst University  
Kansas City, MO 64110, USA  
[matthew.heinrich@rockhurst.edu](mailto:matthew.heinrich@rockhurst.edu)

**Natalie Gerhart**

Department of Business Intelligence and Analytics  
Creighton University  
Omaha, NE 68178, USA  
[NatalieGerhart@creighton.edu](mailto:NatalieGerhart@creighton.edu)

## ABSTRACT

Mobile devices are a constantly used item in a college student's life. Students depend on them for entertainment, academics, and socializing with their friends. While they continually use them, they perhaps do not understand the impact of their use on their privacy or that the devices can be used to track them and collect their personal information. This study utilizes the Antecedent, Privacy Concern, Outcome (APCO) model, combined with the Fogg Behavior Model (FBM) to determine (1) the factors that comprise privacy concerns on a mobile device; (2) whether individuals use privacy-protective behaviors, and (3) whether education on privacy issues regarding mobile devices will increase their use of privacy-enhancing technology (PET). A longitudinal study was conducted to test whether privacy protection education increases the use of PET. While students express concern for their privacy when using mobile devices and express an intent to use additional PET, their behavior using mobile device protections does not change, even after an educational intervention. Perceived privacy control does not change their privacy concern and habit and trust outweigh the impact of privacy concern. Theoretical and practical implications are provided.

**Keywords:** Privacy, Behavioral modeling, IS education, Mobile computing, Intention

## 1. INTRODUCTION

Individuals regularly express concern about privacy in a digital environment, but consistently do little to change behaviors. Data is being collected online at an exponential rate (Lackey, 2019) and mobile devices are now responsible for more than half of all internet traffic (Gaubys, 2021). Many people use their mobile devices to transmit sensitive information, considering these devices just a phone, instead of a pocket computer with the same vulnerabilities as a laptop (Platsis, 2019). Smartphones not only track who you communicate with but also gather less obvious information such as location data, which can determine where you live and work (Obar, 2015). Further, these devices are now an integral part of professional responsibilities, despite limited understanding of the power they wield (Patten & Harris, 2013). Cybersecurity and privacy are of utmost concern in Information Systems (IS) and have led the Society of Information Management's Information Technology (IT) trends study as the top IT management issue from 2017 to 2020 and the IT leader's highest concern from 2014 to 2020 (Kappelman et al., 2020). Data brokers, companies that combine data from multiple sources, make it even more vital for people to understand their data privacy, as this aggregation of data from private and public sources can lead to an in-depth profile of an individual including highly

private information (Acquisti & Gross, 2009). Despite these threats, individuals still engage in risky behaviors. Research considers this phenomenon the privacy paradox (Norberg et al., 2007).

Privacy concern is defined as a user's concern about how their data is being used, and their ability to control that use (Culnan & Armstrong, 1999). Many websites have privacy notices, but this can create a false sense of security for users who believe that a policy implies their data will not be shared (Smith, 2014). Traditionally, privacy control has been left up to users; but more recently, some governments have started to restrict data collection (Information Commissioner's Office, 2019). This signals that users are either not doing enough to protect themselves from dangerous situations, or it is beyond an individual's control. Students operate in an increasingly digital world and need an understanding of the fundamental issues in IS, including privacy and data protection (Harris et al., 2011). Educating users about these data tactics should reduce risky behaviors.

Privacy has been well researched in the IS literature. Individuals who lack technological skills are more likely to be endangered by online privacy issues (Büchi et al., 2017). Privacy education needs to be included in college curricula to prepare students for their eventual careers (Nelson et al., 2011; Park & Vance, 2021). The environment students operate in

increasingly incorporates online education, with 32% of the students having experienced at least one online course (He et al., 2014). With the increased use of online courses, the breadth of applications students are exposed to and expected to use has increased. Along with this increased use, the potential for increased data collection and perhaps data abuse has risen (Lieberman, 2020). Students express privacy concerns, but there is no clear picture of their understanding of the potential danger or ways to mitigate risk (Park & Vance, 2021).

Being aware of the potential for data abuse is only a portion of the problem and may not be sufficient to effectively modify user behavior (Williams et al., 2019). The Fogg Behavioral Model (FBM) identifies three factors that must coalesce to change behaviors: motivation, ability, and a trigger (Fogg, 2009). In short, an individual must be motivated to change a behavior, have the ability to change it, and something must encourage the person to enact that behavioral change. Consequently, this model aids educators to motivate behavioral change for risky behaviors that might be ingrained in the user and offer pedagogical suggestions for increasing privacy awareness in the future workforce.

In this research, we posit that individuals lack awareness of the depth of the data being collected, and the ability to protect themselves on their mobile devices. Further, we posit the need for an external factor (trigger) that encourages users to change their privacy behaviors. We propose the following research problem: Can privacy education impact users' privacy protection behaviors? Specifically, we introduce users to a privacy-enhancing tool (DuckDuckGo), which automatically reduces privacy risks for the user. According to privacy research, the motivation to reduce privacy risks exists for many users (Kokolakis, 2017; Lutz & Strathoff, 2013; Park & Vance, 2021). The ability to control privacy may not exist for a user at the level they perceive (Jensen et al., 2005). We propose that privacy education can serve as a motivator, increase a user's ability to control their privacy, and act as a trigger to change behaviors.

Our findings suggest that the privacy paradox is greater than the impact of the education component. While students express privacy concern and this concern impacts intention and behavior, the educational component offered in this study was insufficient to make a significant impact on privacy concern or behavior. Elements of trust, familiarity, and habit outweighed any increase in privacy awareness. Our findings have important insights for the privacy paradox research stream, as well as an important understanding for users and business owners. Through this research, we further the understanding of the privacy paradox.

The remainder of this paper is organized as follows. First, we outline the related literature on privacy concern, privacy calculus, and the FBM. Next, we develop thirteen hypotheses to explain privacy protection behaviors. The methodology describes the time-series survey, and the results are presented. Finally, we discuss the results and offer contributions, implications, and limitations.

## **2. LITERATURE REVIEW**

### **2.1 Privacy**

Privacy is built on the idea of control; specifically, controlling who can see your personal information (Westin, 1967). Literature has identified four dimensions of privacy: excessive

data collection, errors in collecting data, unauthorized secondary use of data, and improper access to data (Smith et al., 1996). These dimensions have been expanded to include environmental and personal characteristics such as individual control, general privacy concern, trust, and risk beliefs (Malhotra et al., 2004).

As technology has evolved, so has individuals' understanding of privacy, including the impact of mobile devices. Unfortunately, research has not consistently included new technologies, such as mobile devices, when evaluating privacy concerns (Yun et al., 2019). Data collection on mobile devices can be performed continuously and individuals should be encouraged to use protective behavior (Belanger & Crossler, 2019). The Mobile Users Information Privacy Concern (MUIPC) construct includes three concepts: perceived surveillance, or the degree to which an individual believes mobile devices or applications continually monitor behavior; perceived intrusion, or the extent to which an individual believes their personal privacy boundaries are being violated by these devices; and secondary use of information, which is the extent an individual believes their personal information is being shared with others beyond their control (Xu et al., 2012). Limiting data sharing on mobile devices often limits the functionality of the device. For example, turning off location tracking negates the key affordances of a map feature on a mobile device. Likewise, the complexity of technology has made controlling privacy settings more challenging. For example, on mobile devices, each application might require its own privacy settings, which can prove laborious for the user. Similarly, information has varying degrees of privacy concern, based on the perceptions of the user (Malhotra et al., 2004). One individual might find their home address highly sensitive, while others might not care to protect this data.

A factor in determining the value of private information is how it would be used (Smith et al., 1996). Companies benefit from collecting private information because they can use this data to better understand the market, thus creating a competitive advantage. Therefore, companies bolster the need for sharing private information to help the user benefit from personalized messaging (Baruh & Popescu, 2017). In digital settings, it is nearly impossible to know what data will be used, as the combination of the data completed by data brokers greatly enhances the value of the data (Obar, 2015).

Research shows that privacy concerns are enough to prevent users from adopting a technology (Gu et al., 2017) and that application permission requests on a mobile device can increase the privacy concern (Degirmenci, 2020). Privacy concern is often mitigated because of many users' perception that nothing bad will happen to them personally (Jones & Chin, 2015). Further, privacy concern may not be completely understood in the context of peer disclosure in social networks and individuals need additional support in identifying this potential (Alsarkal et al., 2019). In fact, some users show less concern with mobile devices, despite their computing equivalence (Platsis, 2019).

Privacy calculus recognizes that users might have a privacy concern, but performs mental math to determine whether the privacy risk does not outweigh the potential benefits of releasing private information (Dinev & Hart, 2004). Some research avers that the fundamental assumption of privacy calculus does not always hold and despite the stated intentions of not disclosing information, this is not reflected in actual

behavior (Norberg et al., 2007). Research has demonstrated a difference in privacy decisions when measured in different contexts. Hypothetical decisions are more impacted by the objective levels of protection specified by the application/vendor, while actual decisions are more impacted by relative levels of protection measured by personal experience or comparing privacy policies between applications/vendors (Adjerid et al., 2018). Despite this, privacy calculus is dominant, but irrational processes should be considered (Barth & de Jong, 2017). To make rational choices, people have to realize they are making a choice and be capable of making that choice (i.e., enacting privacy protection behaviors) (Masur, 2019).

To make sense of the complexity of privacy calculus research, Smith et al. (2011) developed the Antecedent, Privacy Concern, Outcomes (APCO) framework. This framework identifies the vast amount of research constructs that are good predictors of privacy concern and the breadth of outcomes that can result. Even this cohesive unifying framework has gone through additions to include affective elements, resource constraints, motivations, user biases, and environmental concerns (Dinev et al., 2015). In summary, many factors can reduce privacy concerns or result in users seeming to behave irrationally.

IS literature identifies that behaviors being perceived as irrational could be a result of habit (Heimlich & Ardoin, 2008; Limayem et al., 2007; Polites & Karahanna, 2012). Habit differs from a calculated choice, as it is an automatic reaction created by repetition. Increasing privacy awareness does not override the impact of habit on privacy behavior (Wagner et al., 2020). Concerning IS, habit promotes inertia and resistance to change to a new system (Polites & Karahanna, 2012). “The stronger the habit, the lesser the prognostic power of intention on the actual behavior” (Limayem et al., 2007, p. 730).

## **2.2 Fogg Behavior Model**

The FBM (Fogg, 2009) is a simple model to understand behavioral changes. According to the FBM, motivation, ability, and a trigger must all be present to prompt behavior changes. Fogg (2009) identifies three motivational sources: pleasure/pain, hope/fear, and social acceptance/rejection. Each of these motivations can be seen in privacy research. For example, pleasure could be derived from a user feeling confident about their privacy settings. Alternatively, motivation to protect privacy could be high due to privacy concerns caused by the increased awareness of data collection behaviors in the current climate. Pain could come from a breach of private information. Fear develops from the loss of control and the unknown that results from the breach of private data. Having one’s private information abused results in higher privacy concern (Smith et al., 1996). Finally, social acceptance is an important feature in the adoption and use of technology (Venkatesh et al., 2012). Social networks are built for seeking the approval of peers. External motivations through social norms are an opportunity in privacy research (Li, 2011).

According to the FBM, ability can be encouraged by reducing the amount of time an action takes, the financial cost

for the action and the effort necessary to perform the action, ensuring the alignment of the action with social norms and habits (Fogg, 2009). The ability to adopt privacy protection behaviors could be limited due to the complex nature of the privacy settings and the places that data is collected from (Obar, 2015). Consequently, even if one wants to protect one’s privacy, one might find it difficult to do so (Lehtiniemi & Kortnesniemi, 2017).

The FBM identifies three types of triggers: a spark trigger, which involves a motivation element with a message to perform an action, a facilitator trigger, which identifies how an action can be made simpler, and a signal trigger, which is simply a reminder to perform an action if motivation and ability are already present (Fogg, 2009). In this research, we propose that a spark triggering event will strengthen the motivation and ability to encourage behavior change. To better understand the privacy paradox and the role education can play to increase privacy behaviors, we propose the aforesaid research model (Figure 1).

## **3. HYPOTHESES DEVELOPMENT**

Built on the FBM, we consider motivation, ability, and an educational trigger to assess privacy behaviors. The educational trigger serves as a spark to increase motivation and ability by increasing concerns and providing instructional directions.

### **3.1 Motivation**

The MUIPC construct (Xu et al., 2012) is the most suitable for research regarding privacy concern and mobile devices (Belanger & Crossler, 2019; Degirmenci, 2020). It comprises perceived surveillance or the extent to which a mobile device is monitoring behavior, perceived intrusion, or the extent to which privacy boundaries are being violated by their mobile device, and the secondary use of information, the sharing of personal information with others beyond their personal control.

Privacy experience captures the extent of an individual’s experience with privacy abuse of their data (Benamati et al., 2017). Essentially, one who has had a privacy violation in one’s past person becomes more vigilant to privacy concerns. Unsolicited personalized messages received by an individual can increase the suspicion of unauthorized sharing of their information (Okazaki et al., 2009). Similarly, persons exposed to more privacy breach news are more aware of privacy issues (Benamati et al., 2017). These reports tend to be more massive breaches [i.e., Cambridge Analytica/Facebook (Hern, 2018)], but still drive awareness and therefore more concern. Contrastingly, if a person is unaware of the impacts of private data being used for undesirable purposes, they are less likely to be concerned about their privacy in general. Therefore, we hypothesize:

*H1: Privacy Experience positively relates to mobile users’ information privacy concern.*

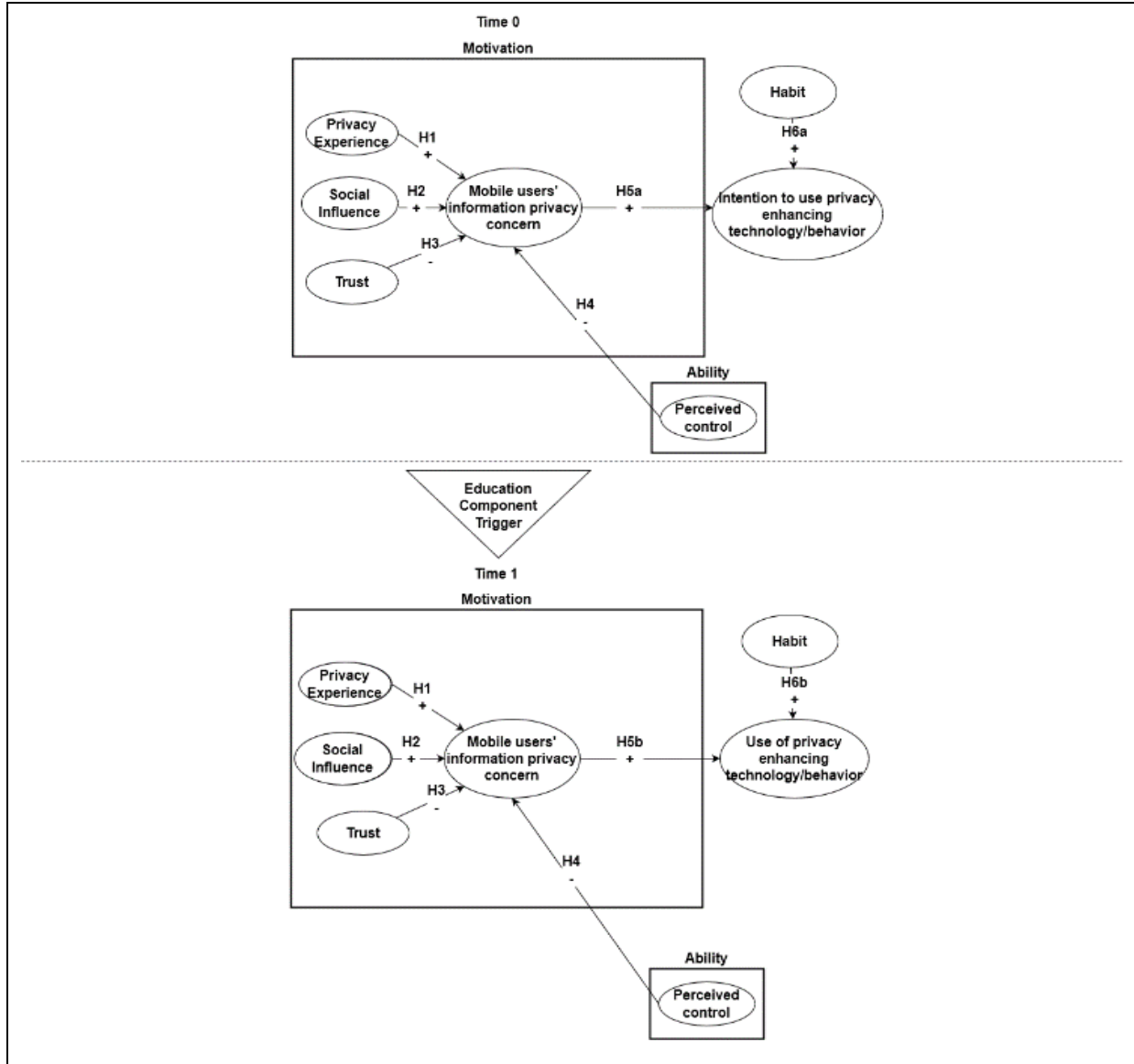


Figure 1. Structural Model

Others' opinions are important in much of the literature relating to technology adoption and use. Social influence is defined as the extent to which an individual is motivated based on the opinion of important others (Venkatesh et al., 2003). It is natural for people to be concerned about issues that concern their role models too. For example, parental privacy concern can be passed on if parents discuss privacy issues with their children (Feng & Xie, 2014; Youn & Shin, 2019). Peers expressing privacy concerns too results in higher individual privacy concerns (Moscardelli & Divine, 2007). Therefore, if influential people are concerned about privacy, a person is more exposed to those privacy concerns and more likely to adopt the concerns in their own beliefs. Consequently, we hypothesize:

*H2: Social influence positively relates to mobile users' information privacy concern.*

Trust is defined as the belief that technology is handling an individual's data properly (Dinev & Hart, 2006). Trust is an important construct in the privacy calculus literature (Dinev & Hart, 2006; Dinev et al., 2015). Trust is so important that some users will not consider participating online if there is no adequate trust (Milne & Boza, 1999). As an individual uses a device more and more and continues to have good experiences, trust in the device grows. Mobile devices are used heavily by youth and provide them a recognizable value that they expect to continue (Hillman & Neustaedter, 2017). Consequently, trust reduces privacy concern (Culnan & Armstrong, 1999; Pavlou et al., 2007; Smith et al., 2011; Xu et al., 2009). Therefore, we hypothesize:

*H3: Trust negatively relates to mobile users' information privacy concern.*

### **3.2 Ability**

Perceived control of personal information is defined as an individual's belief that they can control their personal information (Xu, 2007). On mobile devices, control could exist within privacy settings, such as access to data from an application. Intuitively, for someone to engage in privacy protection behaviors, they first must believe they have control over their privacy. When people believe they are incapable of protecting their privacy, privacy concern is increased (Xu, 2007). Without the ability to control privacy, privacy does not exist (Westin, 1967). Perceived control has been negatively associated with privacy concern in mobile settings (Degirmenci, 2020). Even in situations of greater risk, users with higher perceived ability show reduced privacy concern (Brandimarte et al., 2013). In alignment with prior literature, we hypothesize the following:

*H4: Perceived control negatively influences mobile users' information privacy concern.*

Privacy concerns result in people being more cautious in their actions (Lutz & Strathoff, 2013). For example, users are less likely to download mobile applications if they have a heightened privacy concern (Gu et al., 2017). Users are also less likely to provide private information if privacy concern is greater (Xu et al., 2012). Therefore, as the privacy concern of an individual increases, the individual is more likely to engage in privacy protection behaviors (Osatuyi, 2015; Smith et al., 1996; Stewart & Segars, 2002). Privacy concern can motivate several privacy protection behaviors (Son & Kim, 2008). Therefore, we propose that privacy protection intentions and actions will both be impacted by privacy concern. We hypothesize:

*H5a: Mobile users' information privacy concern positively relates to the intention to use PET.*

*H5b: Mobile users' information privacy concern positively relates to the use of PET.*

### **3.3 Habit**

Per the FBM, motivation and ability can work together in relative weights where sufficient motivation can overcome a lack of ability or *vice versa*, in causing behavioral change (Fogg, 2009). Changing behavior may require a change in habit. Habit is the idea that people have behaviors that become automatic due to repeated experience (Limayem et al., 2007). Habit is a significant indicator in many studies related to the intent or adoption of new technologies (Venkatesh et al., 2012). If people are in the habit of not protecting their privacy, or not using specific technologies, this habit will have to be broken. Similarly, if a user has always used one browser, encouraging the use of a different browser will require changing routines. This can be challenging, even if there is a known risk in continuing their current behavior. Habit also perhaps hampers the use of privacy management tools (Barth & de Jong, 2017). Therefore, we propose that habit has an impact on both intentions and actual behaviors:

*H6a: Habit positively relates to the intention to use PET.*

*H6b: Habit positively relates to the use of PET.*

### **3.4 Trigger**

Prior literature heavily informs privacy concern and privacy protection behaviors; however, there is still confusion about why people express concern and yet do nothing to protect their privacy. This research is built on the idea, based on the FBM, that there needs to be a trigger to spark privacy protection behaviors. This spark should increase both motivation and the ability to result in changing behaviors.

While most users are aware of privacy, data collection, and some uses of data, many are unaware of the depth of these practices (Omoronyia et al., 2013). More specifically, users often do not relate actions directly to the source. Privacy education will make people more aware of the experiences they have had and how privacy protection behaviors could improve their experiences. Enhancing users' awareness of privacy concerns as they are happening increases the desire to change privacy behaviors (Gerber et al., 2018). Consequently, we propose that privacy education, in general, will impact the privacy awareness of users.

*H7: Privacy education will increase privacy experience awareness.*

Making individual users more aware of privacy issues also has an impact on the collective. Privacy education, by the sheer fact, that it exists and is being shared, indicates others are concerned about privacy. As others' concern increases and is reflected in their use of PET, they are more likely to encourage the use of these technologies in their social networks (Mendel & Toch, 2017). Increased use among peers can lead to the development of a social norm where individuals believe that the use of PET is expected (Aarts & Dijksterhuis, 2003). These norms influence action in "direct and meaningful ways" (Schultz et al., 2007, p. 429), highlighting the impact of social influence on intention and behavior. Privacy education will increase perceptions that others believe privacy concern to be important. Therefore, we hypothesize:

*H8: Privacy education will increase social influence awareness.*

Educating users about privacy should bring about related trust concerns for the user. Users indicate increasing privacy concerns if they find data being shared involuntarily (King, 2014). Generally, those with higher education have less trust in companies collecting private data (Wang & Yu, 2015). Mobile devices are complicated and often collect data unbeknownst to the user. Further, the data collected is often not individually useful but gains value, as it is aggregated by data brokers (Federal Trade Commission, 2014). Through education on the ability of organizations to use data, individuals should become more aware of the need to be concerned about privacy. Therefore, we propose the following:

*H9: Privacy education will decrease trust.*

For individuals to change behaviors, they must be capable of doing so (Masur, 2019). Research shows that increased privacy training on social networks increases privacy concerns (Smith et al., 2018). Büchi et al. (2017) demonstrate that

technology skills are the largest predictor of protective behavior. Kulyk et al. (2016) developed guidelines based on expert users to assist others who lack the understanding to protect themselves. By educating users about how privacy can be protected, through new technologies, users should feel empowered by their abilities. Thus, their perception of control over their own privacy should increase.

*H10: Privacy education will increase perceived control.*

MUIPC is a multi-level construct comprised of perceived surveillance, perceived intrusion, and secondary use (Xu et al., 2012). The educational component (Teaching Privacy Project, 2016) contains sections addressing each of these issues. As individuals are educated as to how data is constantly collected through services such as location tracking on their mobile devices, the perception of surveillance should increase. Understanding that data is valuable and can be monetized should increase an individual’s understanding of the potential for unauthorized or unexpected secondary use. As mobile applications continually request access to a variety of information stored on your devices, learning to question whether providing that data is necessary for the functioning of the application should increase the perception of the potential for intrusion into what should be considered private. Collectively, privacy education will increase MUIPC as people become more aware of privacy breaches. As a result, we hypothesize:

*H11: Privacy education will positively impact mobile users’ information privacy concern.*

**4. METHODOLOGY**

Students in select courses at two Midwestern universities were surveyed to measure the impact of an educational component on their use of PET on their mobile devices, in exchange for a small course credit. Surveys were offered online via Qualtrics. A pre-intervention survey established an understanding of existing concern levels and students’ intent to use PET. Next, an educational component consisting of a brief video “You’re leaving footprints” (Teaching Privacy Project, 2016) was provided, which offers an overview of privacy challenges faced in everyday life from video surveillance to location tracking and internet traffic collection. While video surveillance cannot be controlled from an individual’s mobile device, a large amount of the data a student generates is a result of their interaction with their mobile device. Fifty-four percent of the total web traffic is generated from mobile devices (Ceci, 2022). A handout detailing methods to improve their privacy on mobile devices including the use of the DuckDuckGo browser (See Appendix A) was also provided. There are various PET application options available for users to install and protect their data. DuckDuckGo was selected due to its being a single application

that provides a variety of services and is available in both Android and iOS versions. DuckDuckGo does not collect or monetize the history of user searches and blocks known third-party tracking systems (DuckDuckGo, 2008). These third-party systems are not part of the website that a user visits but are provided by a third party to assist in data gathering, both for the website and the business providing the tracker (Emerging Technology from the arXiv, 2014). A post-intervention survey was offered two weeks later.

Scales (See Appendix B) from prior research were adopted. MUIPC is measured with the scale developed by Xu et al. (2012) and adapted to mobile devices rather than mobile applications. Privacy awareness was adapted from the work of Benamati et al. (2017), perceived control of personal information from Xu et al. (2007), social influence from Venkatesh et al. (2012), trust from Dinev and Hart (2006), and habit from Limayem et al. (2007). The intention to use DuckDuckGo was adapted from Venkatesh et al. (2003) and the actual use of DuckDuckGo from Venkatesh et al. (2008).

Four hundred and ninety students were offered participation in the study. 285 students completed the pre-intervention survey and 364 students completed the post-intervention survey. Responses were matched on student ID and only students who completed both surveys were included in the final sample. Attention checks were provided in both surveys and anyone failing either was removed. Participants who completed the post-intervention survey before two weeks or indicated they did not review the educational component were also removed. The final sample size of the matched results was 125 students. Demographic breakdowns of the final sample can be seen in Table 1.

**5. RESULTS**

Partial least squares structural equation modeling (PLS-SEM) was used to analyze the data. This method has the ability to model complex relationships with multiple variables (Chin, 1998). Results were tested using SmartPLS 3.3.3 (Ringle et al., 2014). All constructs except MUIPC were modeled with reflective indicators. MUIPC is a second-order reflective-formative construct of the three dimensions of perceived surveillance, perceived intrusion, and secondary use (Xu et al., 2012). To measure the second-order construct, a two-stage approach was used based on Hair et al. (2014).

**5.1 Instrument validation**

Factors were measured by evaluating reliability, convergent validity, and discriminant validity. Reliability is a measure signifying that indicators consistently represent the measured factor (Hair et al., 2014). During the initial evaluation, an exploratory factor analysis (EFA) using principal axis factoring with Oblimin rotation was performed in R 4.0.5 for both surveys. A confirmatory factor analysis (CFA) in SmartPLS was also used to evaluate reliability and internal consistency.

Age			Gender				Level		
18-20	83	66%	Female	53	42%	Freshman	6	5%	
21-23	34	27%	Male	71	57%	Sophomore	56	46%	
24+	8	6%	Other	1	1%	Junior	34	28%	
						Senior	21	17%	
						Graduate	8	4%	

**Table 1. Demographics**

An indicator for perceived surveillance, a component of MUIPC was excluded from further analysis due to unsatisfactory loading.

Reliability is measured by evaluating the outer loadings of the indicator variables (Hair et al., 2014) to create a composite reliability (CR) score, which should be above 0.7 (Fornell & Larcker, 1981). Construct reliability and validity were evaluated (See Appendix C, Tables C-1 and C-2). The pre-intervention survey results indicated that CR ranged from 0.83 to 0.99 and the post-intervention CR from 0.87 to 0.98. Convergent validity is confirmed if indicators positively correlate with other indicators of the same construct (Hair et al., 2014). This is shown by examining the outer loadings of the indicators and the average variance extracted (AVE) (Hair et al., 2014). Outer loadings should be above 0.708 and AVE should exceed 0.50 (Hair et al., 2014). All factors in both surveys satisfy these criteria. To measure discriminant validity, a factor correlation matrix is utilized. The square root of the AVE of each factor should exceed the correlation between that factor and any other factors (Fornell & Larcker, 1981). This criterion is met, indicating satisfactory discriminant validity.

Common method bias can be problematic in research using surveys (Podsakoff et al., 2003). Harman's single factor test indicated no individual factor exceeded 50% of the variance (Podsakoff et al., 2003). Of the factors that emerged, the largest variance percentage was demonstrated by MUIPC at 26.80% in the pre-intervention survey and 26.93% in the post-intervention survey. Additionally, if all latent variables exhibit a variance inflation factor (VIF) of less than 3.3, the model does not suffer from Common Method Bias (CMB) (Kock, 2015). VIF was measured for the dimensional components of MUIPC and in the final model between all latent variables (See Appendix C, Table

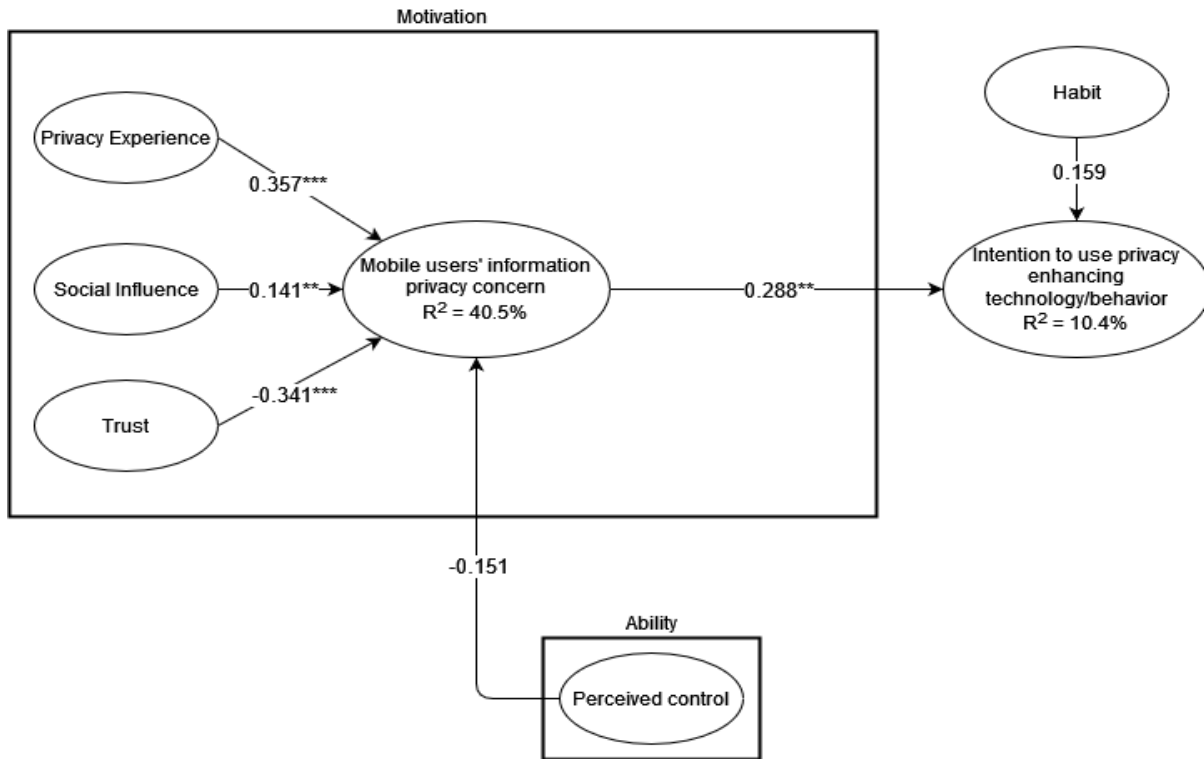
C-3). The maximum VIF was 2.759 in the pre-intervention survey and 2.100 in the post-intervention survey, demonstrating that CMB is not a concern.

**5.2 Structural Model**

The structural model was evaluated by examining the path coefficients and the R<sup>2</sup> values. The results of the analysis of the pre-intervention are shown in Figure 2 and the results of the post-intervention survey after the educational component are depicted in Figure 3. All hypotheses are supported except H4 and H6a.

To evaluate the impact of the educational component, changes in the constructs from pre-intervention to post-intervention were measured following the change model described by Roemer (2016). This is particularly useful for longitudinal data, as the primary desire is to measure changes in the constructs (Roemer, 2016). Paired sample t-tests were performed to evaluate whether changes in the constructs were significant and used to evaluate hypotheses (See Appendix C, Table C-4).

Results were mixed, with full support for H7 and H10. Within social influence, only one of the indicators, S2, showed significant change, providing only partial support for H8. No indicators of trust were impacted, rejecting H9. As MUIPC is a multi-level reflective-formative construct, indicators were compared to determine the impact. No MUIPC indicators changed significantly, rejecting H11. Insufficient change in the level of privacy concern makes it impractical to attempt a comparison between path coefficients in the pre-intervention and post-intervention models (Roemer, 2016). A summary of the hypotheses results is provided in Table 2. The effect sizes for both models were also measured (See Appendix C, Table C-



**Figure 22. Pre-Intervention Survey Model Path Coefficients (\*\*p<0.001; \*\*p<0.05)**



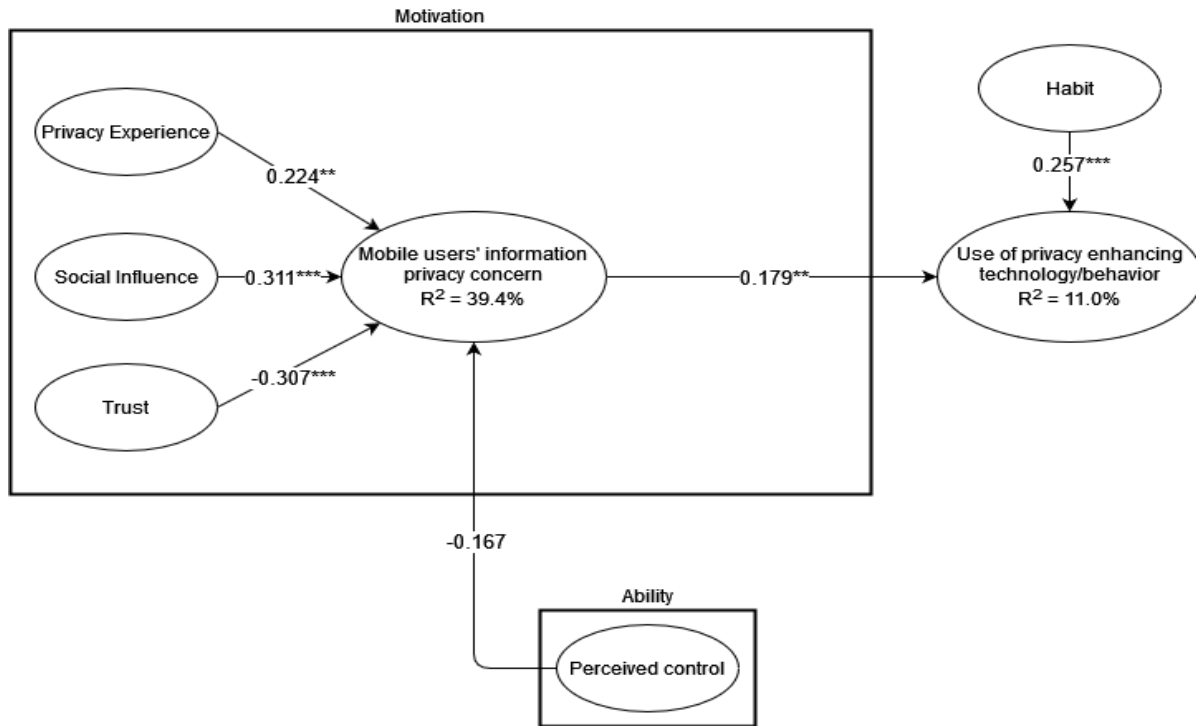


Figure 3. Post-Intervention Survey Model Path Coefficients (\*\* $p < 0.05$ ; \*\*\* $p < 0.001$ )

5) using Cohen's  $f^2$  statistic (Cohen, 1988) and provided a practical measure of impact, regardless of the sample size.

## 6. DISCUSSION

Mobile devices are ubiquitous in the life of current college students, but it is not clear whether they are aware of the potential privacy issues inherent in their use. This study investigates whether an educational component could increase awareness sufficient to impact an individual's privacy concern and in turn lead to an increased use of PET. This research utilized the prior theory of MUIPC (Xu et al., 2012) within the APCO framework (Smith et al., 2011). Guided by FBM (Fogg, 2009), an educational component was offered to determine if sufficient ability and motivation could be attained to cross the threshold of behavior change and increase the use of PET. Consistent with prior research in the APCO model (Smith et al., 2011), this study's results show students do express concern for their privacy while using mobile devices and this concern is impacted by multiple antecedents (Sheehan & Hoy, 2000; Smith et al., 2011; Xu et al., 2012). Privacy concern leads to an intention to use PET and the actual use of PET. The central component of privacy concern was, however, unchanged after the educational component.

Concern for privacy exists at both the pre-intervention and post-intervention surveys. Several antecedents of privacy concern were impacted, but privacy concern did not increase significantly. The use of PET was not significantly impacted. This divergence of intention/use has been shown previously. In a study of information disclosure on social networks, "little to no relationship" (Tufekci, 2008, p. 20) was found between expressed privacy concern and disclosure behavior. In a Facebook study, concern for privacy and knowledge of existing

privacy controls did not impact posting behavior (Reynolds et al., 2011). UTAUT2 (Venkatesh et al., 2012) demonstrated that intention has a positive impact on use, but differences in intentions versus use in this and other studies demonstrate that both outcomes need to be studied. This study measures both intention and use and shows privacy concern impacts both.

Intention precedes behavior and obstacles may exist that could limit use (Bagozzi, 2007). Limayem et al. (2007) demonstrates habit has the potential to completely overcome intention's impact on behavior. Habit has been shown to impact privacy decisions (Wagner et al., 2020) and new technology adoption (Polites & Karahanna, 2012, 2013). In this study, habit demonstrated the most impact after the educational component was delivered. When faced with the need for the actual implementation or continuation of PETs, concern is overridden by the established routine individuals have with their mobile devices. While a calculated decision is contemplated, a paradox still seems to exist between privacy concern when using mobile devices and PET use (Keepsafe, 2018; Norberg et al., 2007).

The educational component and time lag provided interesting results. Privacy awareness increased. This may be a result of having a better understanding of what a privacy breach is. In reviewing personal history, individuals may more accurately identify similar events in their own experience. The impact of social influence on privacy concern also increased, primarily driven by the indicator of people who influence behavior. Feng and Xie (2014) demonstrated that parents' level of concern impacts teens' use of privacy strategies. Additional education for these major influencers may be necessary to promote privacy-protecting behavior. It was hypothesized that an increase in knowledge would reduce the level of trust in mobile devices and therefore limit the negative impact of trust on privacy concern. However, trust was not significantly

Hypotheses	Results
H1: Privacy awareness positively relates to mobile users' information privacy concern.	Supported
H2: Social influence positively relates to mobile users' information privacy concern.	Supported
H3: Trust negatively relates to mobile users' information privacy concern.	Supported
H4: Perceived control negatively influences mobile users' information privacy concern.	Not supported
H5a: Mobile users' information privacy concern positively relates to intention to use PET.	Supported
H5b: Mobile users' information privacy concern positively relates to the use of PET.	Supported
H6a: Habit positively relates to intention to use PET.	Not Supported
H6b: Habit positively relates to the use of PET.	Supported
H7: Privacy education will increase privacy experience awareness.	Supported
H8: Privacy education will increase social influence awareness.	Partially Supported
H9: Privacy education will decrease trust.	Not supported
H10: Privacy education will increase perceived control.	Supported
H11: Privacy education will positively impact mobile users' information privacy concern.	Not Supported

**Table 2. Hypotheses Results**

changed after the educational component. This was an unexpected outcome. Familiarity builds trust (Gefen, 2000) and it may be that the high level of familiarity the sample had with their mobile devices outweighed the impact of the education component. Trust has been established as a central component of technology adoption (Gefen et al., 2003). Venkatesh et al. (2012) indicate that trust plays a larger role in the actual use of technology than intention. Device vendors understand the need to establish trust to promote use. Gefen et al. (2003) refer to structural assurances or safeguards included in the design of technologies that promote trust. Apple and Android both extensively promote the safety and privacy of their devices (Android Support, n.d.; Apple Support, 2021). Even though individuals become increasingly aware of the potential risks of using mobile technologies, their trust in these platforms outweighs this increasing risk level.

In the context of the FBM (Fogg, 2009) motivation and ability are both necessary to permit a behavioral change. Motivation measured by MUIPC remained relatively constant at the pre-intervention and post-intervention stages. Perceived control increased from the pre-intervention to post-intervention stage but had an insignificant impact on privacy concern. Individuals may feel they have additional control, but as Obar (2015) points out, the explosion of data, data gathering and aggregation may make it impossible for an individual to exert control over all their private data. "In the cold light of experience, the digital citizen knows that data privacy self-management is a fiction." (Obar, 2015, p. 1).

Not all hypotheses were accepted but it does appear that education can impact the consideration process of privacy calculus. This study supports privacy calculus, as intention and use are impacted by concern. Interestingly, the privacy paradox is also represented in the fact that concern was not increased, though antecedents to privacy concern were.

**6.1 Theoretical contributions**

This study makes two primary contributions to ongoing theory. Firstly, to our knowledge no paper has analyzed privacy behavior based on the FBM (Fogg, 2009). FBM is a persuasive model designed to be used to modify behavior. FBM has been used in the design of IS but has not been applied to behavioral change regarding privacy protection. Its relationships between ability, motivation, and triggering events provides a good theoretical basis to evaluate the impact of education on PET

use. A continuing effort to find the correct mix of motivator, ability, and trigger mechanisms should prove fruitful.

Privacy calculus is strengthened through replicating tests of antecedent impact on privacy concern and the outcome of intention to use and actual use of PET. Concomitantly, the privacy paradox theory is advanced as demonstrated by increases in privacy concern antecedents not impacting actual use. Paradoxical patterns continue to emerge, even from college students who have grown up as digital natives (Prensky, 2001). Even though they have been raised in an environment of advanced technologies and may be perceived as having a better understanding of technology, their use of PET is not equivalent to their expressed level of privacy concern. (Kurkovsky & Syta, 2010).

Further, this study provides insight into potential obstacles to the adoption of PET. Trust and habit remain powerful barriers to change, as students use but perhaps lack understanding of all the technical aspects of their devices. Constant use of these devices builds familiarity and therefore trust (Gefen, 2000). Lacking the perception of control over their devices, habits dominate their management of their mobile devices.

Finally, this study demonstrates a potential behavior gap that may prove detrimental to students as they move beyond academia. Students need an understanding of the impact of privacy in their use of mobile devices, as they are an ever-increasing portion of their lives both personally and professionally. Currently, we are not aware of any educational research that has assumed the task of educating students to lessen the privacy paradox they demonstrate.

**6.2 Practical implications**

Practical implications are also demonstrated by this study. Even though current students can be considered digital natives and are aware of potential privacy issues, their use of PET does not seem to be impacted. Organizations are constantly threatened with attacks and potential data leakage (Patten & Harris, 2013). Upon these students' entry into the workforce, organizations need to realize they may not be active in protecting data and may pose a security risk. Personal mobile devices continue to expand in the workplace. Awareness of threats will need to be constantly assessed and stricter policies on personal device use may need to be implemented. The constant use of these devices over their lifetime and the resulting established habits may

increase the risk companies face. Individuals in this study demonstrate privacy concern but did not increase their use of PET to safeguard their personal information. Not acting to protect their own information more substantially indicates they may not try to protect information that belongs to the businesses they work for.

For educators, this study demonstrates the need for educating students of the potential risks mobile devices involve and the harm they might experience due to a lack of protection. Excessive sharing and lack of privacy protection of their private information can have long-lasting damaging effects, which may not be fully understood (Baruh & Popescu, 2017). A brief educational intervention was able to increase their awareness of privacy issues but was insufficient to enact behavioral change. Education at all levels, perhaps most importantly early in their use of these devices before trust is established and habits formed, is necessary to prepare students for the dangers they may face. Early education should also include those primary influencers of behavior including parents and guardians, especially when their influence may be greater (Feng & Xie, 2014).

For regulators, this study demonstrates the need for legislation to protect private information on mobile devices. Inattention, habit, and misplaced trust in private information being shared unintentionally. Device manufacturers and application developers could use privacy protection as a way to increase sales as consumers continue to express privacy concern. For example, Apple Inc. has recently started requiring “privacy labels” on applications distributed via their online store (Newman, 2020). This process, combined with Apple’s intention to add to its operating system the ability to block tracking, is already causing a stir in the online advertising and social media markets (Wong, 2021). DuckDuckGo has surpassed 100 million daily searches (Cimpanau, 2021). Clearly, there is a market for privacy-related consumer technologies. Companies should continue to increase the usefulness and ease of use of these devices and applications to encourage easier and wider adoption.

## **7. LIMITATIONS AND FUTURE RESEARCH**

Consistent with all research, there are several important limitations to this study. This study was conducted across multiple institutions of higher education, but the student profiles are similar, and the results may not be generalizable to all populations. Graduate and undergraduate students in various stages of their academic career were surveyed to limit the homogeneity of the sample, but this remains a small population and may not be generalizable to a wider audience. Future research should consider the impact of education on privacy protection behaviors in other contexts outside of the classroom.

Privacy research is extensive (i.e., the APCO framework) (Smith et al., 2011), suggesting that other antecedents or outcomes should be included to better understand the impact of educational components on privacy concern and behaviors. For example, DuckDuckGo does not save a history of search terms. This could limit the potential for more targeted searching based on user history to provide improved results. This limitation could negatively impact perceived usefulness and limit adoptions. Not storing passwords or “fireproofing” sites in DuckDuckGo requires the reentry of credentials each time a site is visited potentially limiting perceived ease of use and again

limiting adoption. This study is the first application of FBM to privacy education. As such, a starting point needed to be determined. Further research using DuckDuckGo or other applications is needed. While this study considers intention and use of PET, additional outcome variables could be evaluated to better understand these relationships.

Additional limitations in this study indicate the need for further research. When evaluating the MUIPC construct sub-components (Xu et al., 2012) perceived surveillance did not factor as expected. Privacy concern scales have evolved over time from CFIP (Smith et al., 1996) and UIPC (Malhotra et al., 2004) to the mobile environment with MUIPC. MUIPC may need to be reevaluated in the current technology environment extending the privacy concern scale again. Privacy here is studied as a general concept. An improved understanding of what information students classify as private could also provide additional guidance in developing motivational and educational materials for the adoption of PET. Additional work could be done to determine different boundaries individuals place on different elements of their personal information. Prior research has also indicated this need to classify what is considered private (Clarke, 1999; Malhotra et al., 2004; Solove, 2008). Information should be segmented based on an individual’s perception of what they believe should remain private. The disconnect between intention and use deserves more study. Knowledge of what limitations or barriers cause individuals not to behave in a manner consistent with their concerns could guide those in the practical application of legislation, application creation, or curriculum.

This study introduced motivation by attempting to increase the fear level individuals have regarding protection of their information. There may be better approaches as fear may also lead to a feeling of being overwhelmed by the task of protecting their privacy. The educational component may have provided some increased knowledge of relatively simply protection tasks but a broader approach to different motivational and ability components could have a larger impact on behavior modification. Awareness levels of privacy issues increased in this study. Perceptions of control, however, did not impact privacy concern at either pre-intervention or post-intervention. Lack of a sufficient mechanism for addressing fear could have resulted in inaction or habitual behavior.

Only a brief educational component was utilized in this study. A short video “You’re leaving footprints” (Teaching Privacy Project, 2016) and a handout providing information on DuckDuckGo and basic security options available in Apple and Android mobile environments (see Appendix A) were provided. Our results indicate that no significant change in privacy concern resulted from this educational component. A more substantial demonstration of the potential for privacy invasion via a mobile device, perhaps by targeting the mobile applications students commonly use, could prove more effective. Extending this to a longer, more in-depth, or repetitive process could also provide educators with guidance on more effective educational materials. Per FBM, change is easier to enact when the tasks are simple. Starting with individual easy steps and then building on those may be more effective. Further, the gap between surveys was only two weeks. This does not allow consideration of the potential longer-term impact of an educational component intervention. Future research should consider a longer timeframe, potentially with additional survey points, to better evaluate whether

increased use of the PET grows and forms a habit which would suggest lasting behavioral change. It is conceivable individuals feel controlling their private information is a hopeless cause regardless of their level of knowledge or ability. Future research could investigate potential feelings of hopelessness and provide additional insight theoretically and practically.

Finally, the FBM (Fogg, 2009) could be extended to areas beyond information and PET. FBM has been used in IS design and could be utilized to design education of a repetitive nature delivered by the mobile device itself. The FBM could also be used to explore other behaviors of students to better explain how students consider, adopt, and engage with technology for educational needs.

## 8. CONCLUSION

Technology has and will continue to advance at a tremendous pace. The increased ability to gather, aggregate, and analyze data is a continuing concern for individuals and organizations. Organizations want to provide improved customer services and protect their data. Individuals also request these improved services but may be inadequately informed on the ramifications of sharing data to receive these services. The mobile devices we use constantly can monitor our behavior to provide these improved services but also have the potential to be used for unwanted data collection. The FBM provides an interesting theoretical lens to investigate the interaction between these competing forces and how behavior when using mobile devices can be directed. FBM can provide an additional context to evaluate technology adoption including PET. This study demonstrates that increasing the knowledge and awareness of privacy concerns combined with training on how to alleviate those concerns can have an impact on individual privacy concern and its antecedents.

## 9. REFERENCES

Aarts, H., & Dijksterhuis, A. (2003). The Silence of the Library: Environment, Situational Norm, and Social Behavior. *Journal of Personality and Social Psychology*, 84(1), 18-28. <https://doi.org/10.1037/0022-3514.84.1.18>

Acquisti, A., & Gross, R. (2009). Predicting Social Security Numbers From Public Data. *Proceedings of the National Academy of Sciences of the United States of America*, 106(27), 10975-10980. <https://doi.org/10.1073/pnas.0904891106>

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the Privacy Paradox: Objective versus Relative Risk in Privacy Decision Making. *MIS Quarterly*, 42(2), 465-488. <https://doi.org/10.25300/MISQ/2018/14316>

Alsarkal, Y., Zhang, N., & Xu, H. (2019). Protecting Privacy on Social Media: Is Consumer Privacy Self-Management Sufficient? *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 4875-4884. <https://doi.org/10.24251/hicss.2019.587>

Android Support. (n.d.). *Safety Center - Mobile Safety | Android*. <https://www.android.com/safety/>

Apple Support. (2021). *Apple Platform Security - Apple Support*. <https://support.apple.com/guide/security/welcome/web>

Bagozzi, R. (2007). The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. *Journal of the*

*Association for Information Systems*, 8(4), 244-254. <https://doi.org/10.17705/1jais.00122>

Barth, S., & de Jong, M. D. T. (2017). The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review. *Telematics and Informatics*, 34(7), 1038-1058. <https://doi.org/10.1016/j.tele.2017.04.013>

Baruh, L., & Popescu, M. (2017). Big Data Analytics and the Limits of Privacy Self-Management. *New Media and Society*, 19(4), 579-596. <https://doi.org/10.1177/1461444815614001>

Belanger, F., & Crossler, R. E. (2019). Dealing with Digital Traces: Understanding Protective Behaviors on Mobile Devices. *Journal of Strategic Information Systems*, 28(1), 34-49. <https://doi.org/10.1016/j.jsis.2018.11.002>

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An Empirical Test of an Antecedents - Privacy Concerns - Outcomes Model. *Journal of Information Science*, 43(5), 583-600. <https://doi.org/10.1177/0165551516653590>

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, 4(3), 340-347. <https://doi.org/10.1177/1948550612455931>

Büchi, M., Just, N., & Latzer, M. (2017). Caring Is Not Enough: The Importance of Internet Skills for Online Privacy Protection. *Information Communication and Society*, 20(8), 1261-1278. <https://doi.org/10.1080/1369118X.2016.1229001>

Ceci, L. (2022). *Mobile Internet Usage Worldwide - Statistics & Facts*. Statista. <https://www.statista.com/topics/779/mobile-internet/#dossierKeyfigures>

Chin, W. W. (1998). Issues and Opinion on Structural Equation Modeling. *MIS Quarterly*, 22(1), 1.

Cimpanau, C. (2021). *DuckDuckGo Surpasses 100 Million Daily Search Queries for the First Time*. Zero Day. [https://www.zdnet.com/google-amp/article/duckduckgo-surpasses-100-million-daily-search-queries-for-the-first-time/?tag=COS-05-10aaa0g&taid=6003a4b3947f630001ccbaf&utm\\_campaign=trueAnthem%3A\\_Trending\\_Content&utm\\_medium=trueAnthem&utm\\_source=twitter&\\_twi](https://www.zdnet.com/google-amp/article/duckduckgo-surpasses-100-million-daily-search-queries-for-the-first-time/?tag=COS-05-10aaa0g&taid=6003a4b3947f630001ccbaf&utm_campaign=trueAnthem%3A_Trending_Content&utm_medium=trueAnthem&utm_source=twitter&_twi)

Clarke, R. (1999). Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the Association for Computing Machinery*, 42(2), 60-67.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences*. Lawrence Erlbaum Associates.

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10(1), 104-115. <https://doi.org/10.1287/orsc.10.1.104>

Degirmenci, K. (2020). Mobile Users' Information Privacy Concerns and the Role of App Permission Requests. *International Journal of Information Management*, 50, 261-272. <https://doi.org/10.1016/j.ijinfomgt.2019.05.010>

Dinev, T., & Hart, P. (2004). Internet Privacy Concerns and Their Antecedents -Measurement Validity and a Regression Model. *Behaviour and Information Technology*, 23(6), 413-422. <https://doi.org/10.1080/01449290410001715723>

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus

- Model for E-Commerce Transactions. *Information Systems Research*, 17(1), 61-80. <https://doi.org/10.1287/isre.1060.0080>
- Dinev, T., McConnell, A., & Smith, H. (2015). Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the “APCO” Box. *Information Systems Research*, 26(4), 639-655. <https://doi.org/10.1287/isre.2015.0600>
- DuckDuckGo. (2008). *Privacy, Simplified. DuckDuckGo Browser Extension & Mobile App*. <https://duckduckgo.com/app>
- Emerging Technology from the arXiv. (2014). *The Murky World of Third Party Web Tracking*. <https://www.technologyreview.com/2014/09/12/171400/th-e-murky-world-of-third-party-web-tracking/>
- Federal Trade Commission. (2014). *Data Brokers A Call for Transparency and Accountability*. <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>
- Feng, Y., & Xie, W. (2014). Teens’ Concern for Privacy When Using Social Networking Sites: An Analysis of Socialization Agents and Relationships with Privacy-Protecting Behaviors. *Computers in Human Behavior*, 33, 153-162. <https://doi.org/10.1016/j.chb.2014.01.009>
- Fogg, B. (2009). A Behavior Model for Persuasive Design. *ACM International Conference Proceeding Series*, 350. <https://doi.org/10.1145/1541948.1541999>
- Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18(1), 39-50.
- Gaubys, J. (2021). *What Percentage of Internet Traffic Is Mobile?* <https://www.oberlo.com/statistics/mobile-internet-traffic>
- Gefen, D. (2000). E-Commerce: The Role of Familiarity and Trust. *Omega The International Journal of Management Science*, 28(6), 725-737. [https://doi.org/10.1016/S0305-0483\(00\)00021-9](https://doi.org/10.1016/S0305-0483(00)00021-9)
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly*, 27(1), 51-90. <https://doi.org/10.1017/CBO9781107415324.004>
- Gerber, N., Gerber, P., Drews, H., Kirchner, E., Schlegel, N., Schmidt, T., & Scholz, L. (2018). FoxIT: Enhancing Mobile Users’ Privacy Behavior by Increasing Knowledge and Awareness. *ACM International Conference Proceeding Series*. <https://doi.org/10.1145/3167996.3167999>
- Gu, J., Xu, Y. (Calvin), Xu, H., Zhang, C., & Ling, H. (2017). Privacy Concerns for Mobile App Download: An Elaboration Likelihood Model Perspective. *Decision Support Systems*, 94, 19-28. <https://doi.org/10.1016/j.dss.2016.10.002>
- Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2014). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. SAGE Publications.
- Harris, A., Lang, M., Yates, D., & Kruck, S. E. (2011). Incorporating Ethics and Social Responsibility in IS Education. *Journal of Information Systems Education*, 22(3), 183-190. <https://aisel.aisnet.org/jise/vol22/iss3/1>
- He, W., Xu, G., & Kruck, S. E. (2014). Online IS Education for the 21st Century. *Journal of Information Systems Education*, 25(2), 101-105.
- Heimlich, J. E., & Ardoin, N. M. (2008). Understanding Behavior to Understand Behavior Change: A Literature Review. *Environmental Education Research*, 14(3), 215-237. <https://doi.org/10.1080/13504620802148881>
- Hern, A. (2018). *Far More Than 87m Facebook Users Had Data Compromised, MPs Told*. The Guardian. <https://www.theguardian.com/uk-news/2018/apr/17/facebook-users-data-compromised-far-more-than-87m-mps-told-cambridge-analytica>
- Hillman, S., & Neustaedter, C. (2017). Trust and Mobile Commerce in North America. *Computers in Human Behavior*, 70, 10-21. <https://doi.org/10.1016/j.chb.2016.12.061>
- Information Commissioner’s Office. (2019). *GDPR One year on*. <https://ico.org.uk/media/about-the-ico/documents/2614992/gdpr-one-year-on-20190530.pdf>
- Jensen, C., Potts, C., & Jensen, C. (2005). Privacy Practices of Internet Users: Self-Reports versus Observed Behavior. *International Journal of Human Computer Studies*, 63(1-2), 203-227. <https://doi.org/10.1016/j.ijhcs.2005.04.019>
- Jones, B. H., & Chin, A. G. (2015). On the Efficacy of Smartphone Security: A Critical Analysis of Modifications in Business Students’ Practices over Time. *International Journal of Information Management*, 35(5), 561-571. <https://doi.org/10.1016/j.ijinfomgt.2015.06.003>
- Kappelman, L., McLean, E., Johnson, V., Torres, R., Maurer, C., Snyder, M., Kim, K., & Guerra, K. (2020). The 2020 SIM IT Issues and Trends Study. *MIS Quarterly Executive*, 20(1), 56. <http://www.simnet.org/IT-Trends>
- Keepsafe. (2018). *New Keepsafe Survey Shows The Privacy Paradox Lives On*. <https://www.getkeepsafe.com/blog/new-keepsafe-survey-shows-the-privacy-paradox-lives-on/>
- King, J. (2014). How Come I’m Allowing Strangers to Go Through My Phone? Smartphones and Privacy Expectations. *SSRN Electronic Journal*, March, 1-14. <https://doi.org/10.2139/ssrn.2493412>
- Kock, N. (2015). Common Method Bias in PLS-SEM: A Full Collinearity Assessment Approach. *International Journal of E-Collaboration*, 11(4), 1-10.
- Kokolakis, S. (2017). Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. *Computers and Security*, 64, 122-134. <https://doi.org/10.1016/j.cose.2015.07.002>
- Kulyk, O., Gerber, P., El Hanafi, M., Reinheimer, B., Renaud, K., & Volkamer, M. (2016). Encouraging Privacy-Aware Smartphone App Installation: What Would the Technically-Adept Do. *Usable Security Workshop, February*. <https://doi.org/10.14722/usec.2016.23016>
- Kurkovsky, S., & Syta, E. (2010). Digital Natives and Mobile Phones: A Survey of Practices and Attitudes about Privacy and Security. *2010 IEEE International Symposium on Technology and Society*, 441-449. <https://doi.org/10.1109/ISTAS.2010.5514610>
- Lackey, D. (2019). *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*. <https://blazon.online/data-marketing/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/>

- Lehtiniemi, T., & Kortenesniemi, Y. (2017). Can the Obstacles to Privacy Self-Management Be Overcome? Exploring the Consent Intermediary Approach. *Big Data and Society*, 4(2), 1-11. <https://doi.org/10.1177/2053951717721935>
- Li, Y. (2011). Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*, 28(1), 453-496. <https://doi.org/10.17705/1cais.02828>
- Lieberman, M. (2020). *Massive Shift to Remote Learning Prompts Big Data Privacy Concerns*. Education Week. <https://www.edweek.org/technology/massive-shift-to-remote-learning-prompts-big-data-privacy-concerns/2020/03>
- Limayem, M., Hirt, S. G., & Cheung, C. M. K. (2007). How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance. *MIS Quarterly*, 31(4), 705-737. <https://doi.org/10.2307/25148817>
- Lutz, C., & Strathoff, P. (2013). Privacy Concerns and Online Behavior - Not so Paradoxical After All?: Viewing the Privacy Paradox through Different Theoretical Lenses. In S. Brändli (Ed.), *Multinationale Unternehmen und Institutionen im Wandel - Herausforderungen für Wirtschaft, Recht und Gesellschaft* (Issue Bd. 8, pp. 81-99). Stämpfli Verlag. <https://www.alexandria.unisg.ch/228096/>
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 336-355. <https://doi.org/10.1287/isre.1040.0032>
- Masur, P. (2019). *Reconceptualizing Online Privacy Literacy*. <https://philippmasur.de/blog/2019/03/28/reconceptualizing-online-privacy-literacy/>
- Mendel, T., & Toch, E. (2017). Susceptibility to Social Influence of Privacy Behaviors: Peer versus Authoritative Sources. *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*, 581-593. <https://doi.org/10.1145/2998181.2998323>
- Milne, G. R., & Boza, M.-E. (1999). Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices. *Journal of Interactive Marketing*, 13(1), 5-24. [https://doi.org/10.1002/\(SICI\)1520-6653\(199924\)13:1<5::AID-DIR2>3.0.CO;2-9](https://doi.org/10.1002/(SICI)1520-6653(199924)13:1<5::AID-DIR2>3.0.CO;2-9)
- Moscardelli, D. M., & Divine, R. (2007). Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships with Privacy-Protecting Behaviors. *Family and Consumer Sciences Research Journal*, 35(3), 232-252. <https://doi.org/10.1177/1077727X06296622>
- Nelson, K., Courier, M., & Joseph, G. W. (2011). Teaching Tip An Investigation of Digital Literacy Needs of Students. *Journal of Information Systems Education*, 22(2), 95-109.
- Newman, L. H. (2020). *Apple's App "Privacy Labels" Are Here—and They're a Big Step Forward*. Wired. <https://www.wired.com/story/apple-app-privacy-labels/>
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, 41(1), 100-126. <https://doi.org/10.1111/j.1745-6606.2006.00070.x>
- Obar, J. A. (2015). Big Data and The Phantom Public: Walter Lippmann and the Fallacy of Data Privacy Self-Management. *Big Data and Society*, 2(2), 1-16. <https://doi.org/10.1177/2053951715608876>
- Okazaki, S., Li, H., & Hirose, M. (2009). Consumer Privacy Concerns and Preference for Degree of Regulatory Control: A Study of Mobile Advertising in Japan. *Journal of Advertising*, 38(4), 63-77. <https://doi.org/10.2753/JOA0091-3367380405>
- Omoronyia, I., Cavallaro, L., Salehie, M., Pasquale, L., & Nuseibeh, B. (2013). Engineering Adaptive Privacy: On the Role of Privacy Awareness Requirements. *2013 35th International Conference on Software Engineering (ICSE)*, 632-641. <https://doi.org/10.1109/ICSE.2013.6606609>
- Osatuyi, B. (2015). Is Lurking an Anxiety-Masking Strategy on Social Media Sites? The Effects of Lurking and Computer Anxiety on Explaining Information Privacy Concern on Social Media Platforms. *Computers in Human Behavior*, 49, 324-332. <https://doi.org/10.1016/j.chb.2015.02.062>
- Park, J., & Vance, A. (2021). *Data Privacy in Higher Education: Yes, Students Care*. Educause Review. <https://er.educause.edu/articles/2021/2/data-privacy-in-higher-education-yes-students-care>
- Patten, K. P., & Harris, M. A. (2013). The Need to Address Mobile Device Security in the Higher Education IT Curriculum. *Journal of Information Systems Education*, 24(1), 41-52.
- Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. *MIS Quarterly*, 31(1), 105-136. <https://doi.org/10.2307/25148783>
- Platsis, G. (2019). *Mobile Security Versus Desktop and Laptop Security: Is There Even a Difference Anymore?* <https://securityintelligence.com/mobile-security-versus-desktop-and-laptop-security-is-there-even-a-difference-anymore/>
- Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology*, 88(5), 879-903. <https://doi.org/10.1037/0021-9010.88.5.879>
- Polites, G. L., & Karahanna, E. (2012). Shackled to the Status Quo: The Inhibiting Effects of Incumbent System Habit, Switching Costs, and Inertia on New System Acceptance. *MIS Quarterly*, 36(1), 21-42. <https://doi.org/10.2307/41410404>
- Polites, G. L., & Karahanna, E. (2013). The Embeddedness of Information Systems Habits in Organizational and Individual Level Routines: Development and Disruption. *MIS Quarterly*, 37(1), 221-246.
- Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1. *On the Horizon*, 9(5), 1-6. <https://doi.org/10.1108/10748120110424816>
- Reynolds, B., Venkatanathan, J., Gonçalves, J., & Kostakos, V. (2011). *Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours BT - Human-Computer Interaction - INTERACT 2011* (P. Campos, N. Graham, J. Jorge, N. Nunes, P. Palanque, & M. Winckler (eds.); pp. 204-215). Springer Berlin Heidelberg.
- Ringle, C. M., Silva, D. da, & Bido, D. de S. (2014). Structural Equation Modeling with the Smartpls. *Revista Brasileira de Marketing*, 13(2), 56-73. <https://doi.org/10.5585/remark.v13i2.2717>

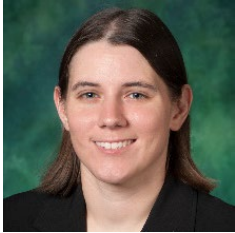
- Roemer, E. (2016). A Tutorial on the Use of PLS Path Modeling in Longitudinal Studies. *Industrial Management and Data Systems*, 116(9), 1901-1921. <https://doi.org/10.1108/IMDS-07-2015-0317>
- Schultz, P. W., Nolan, J. M., Cialdini, R. B., Goldstein, N. J., & Griskevicius, V. (2007). The Constructive, Destructive, and Reconstructive Power of Social Norms. *Psychological Sciences*, 18(5), 429-434.
- Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of Privacy Concern among Online Consumers. *Journal of Public Policy and Marketing*, 19(1), 62-73. <https://doi.org/10.1509/jppm.19.1.62.16949>
- Smith, A. (2014). *Half of Online Americans Don't Know What a Privacy Policy Is*. <https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/>
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4), 989-1015. <https://doi.org/10.2307/41409970>
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20(2), 167-196. <https://doi.org/10.2307/249477>
- Smith, K. H., Mediavilla, F. A. M., & White, G. L. (2018). The Impact of Online Training on Facebook Privacy. *Journal of Computer Information Systems*, 58(3), 244-252. <https://doi.org/10.1080/08874417.2016.1233001>
- Solove, D. J. (2008). *Understanding Privacy* (Issue May). [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1127888](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888)
- Son, J. Y., & Kim, S. S. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly*, 32(3), 503-529. <https://doi.org/10.2307/25148854>
- Stewart, K. A., & Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, 13(1), 36-49. <https://doi.org/10.1287/isre.13.1.36.97>
- Teaching Privacy Project. (2016). *You're Leaving Footprints*. <https://teachingprivacy.org/module-1-youre-leaving-footprints/>
- Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*, 28(1), 20-36. <https://doi.org/10.1177/0270467607311484>
- Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions Subject Areas: Design Characteristics, Interventions. *Decision Sciences*, 39(2), 273-315. [http://www.vvenkatesh.com/wp-content/uploads/2015/11/Venkatesh\\_Bala\\_DS\\_2008.pdf](http://www.vvenkatesh.com/wp-content/uploads/2015/11/Venkatesh_Bala_DS_2008.pdf)
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3), 425-478. <https://doi.org/10.2307/30036540>
- Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly*, 36(1), 157-178. <https://doi.org/10.2307/41410412>
- Wagner, C., Trenz, M., & Veit, D. (2020). How Do Habit and Privacy Awareness Shape Privacy Decisions? *26th Americas Conference on Information Systems, AMCIS 2020*, 1-10.
- Wang, Z., & Yu, Q. (2015). Privacy Trust Crisis of Personal Data in China in the Era of Big Data: The Survey and Countermeasures. *Computer Law and Security Review*, 31(6), 782-792. <https://doi.org/10.1016/j.clsr.2015.08.006>
- Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.
- Williams, M., Nurse, J. R. C., & Creese, S. (2019). Smartwatch Games: Encouraging Privacy-Protective Behaviour in a Longitudinal Study. *Computers in Human Behavior*, 99, 38-54. <https://doi.org/10.1016/j.chb.2019.04.026>
- Wong, Q. (2021). *Facebook vs. Apple: Here's What You Need to Know about Their Privacy Feud*. Cnet. <https://www.cnet.com/news/facebook-vs-apple-heres-what-you-need-to-know-about-their-privacy-feud/>
- Xu, H. (2007). The Effects of Self-Construal and Perceived Control on Privacy Concerns. In the *28th International Conference on Information Systems, ICIS 2007*. <http://www.scopus.com/inward/record.url?scp=84870960533&partnerID=8YFLogxK>
- Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring Mobile Users' Concerns for Information Privacy. *International Conference on Information Systems, ICIS 2012*, 3(Ftc 2009), 2278-2293.
- Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2009). The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information Systems*, 26(3), 135-174. <https://doi.org/10.2753/MIS0742-1222260305>
- Youn, S., & Shin, W. (2019). Teens' Responses to Facebook Newsfeed Advertising: The Effects of Cognitive Appraisal and Social Influence on Privacy Concerns and Coping Strategies. *Telematics and Informatics*, 38, 30-45. <https://doi.org/10.1016/j.tele.2019.02.001>
- Yun, H., Lee, G., & Kim, D. J. (2019). A Chronological Review of Empirical Research on Personal Information Privacy Concerns: An Analysis of Contexts and Research Constructs. *Information & Management*, 56(4), 570-601. <https://doi.org/10.1016/j.im.2018.10.001>

**AUTHOR BIOGRAPHIES**

**Matt Heinrich** is a clinical assistant professor of business intelligence and analytics at Rockhurst University. He received his DBA from Creighton University. He also holds an Executive MBA and a Bachelor of Professional Studies in Computer Technology, both from Rockhurst University. His research interests include privacy, technology adoption, and data literacy.



**Natalie Gerhart** is an associate professor of business intelligence and analytics at Creighton University. She received her Ph.D. from the University of North Texas. She also holds an MBA from the University of Missouri-Columbia in Marketing Analytics and a Bachelor of Science degree from Truman State University in Management Information Systems and Marketing. Previously, she has published in journals such as *Journal of Management Information Systems*, *Information Systems Journal*, *Decision Support Systems*, and *The DATA BASE for Advances in Information Systems*. Her research interests include decision stopping rules, human computer interaction (HCI), business intelligence and analytics (BI&A), and social networking.





## APPENDICES

### Appendix A. Educational Component Introduction

Please watch the video from teachingprivacy.org linked here <https://teachingprivacy.org/youre-leaving-footprints/>.

#### Improving privacy protection on your mobile device



<https://duckduckgo.com/>

**A browser application for your device (Android or iOS) that provides several layers of protection. Available at the play or app store for your device.**

- Search history is not stored
- Stops tracking cookies
- Forces encrypted connection
- Displays privacy “grades” for websites

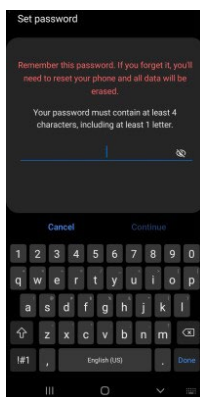
For most browsers, when you search for items on the web using google, Bing, yahoo, etc. all of your searches are stored. This search history is then sold to other vendors. While there are times this can be an advantage as these historic searches can predict what you might be looking for there are also disadvantage. If you’re searching for private information, such as health information, it may be better to not have those stored.

Cookies are small files that are installed on your device when you visit a website. They are used to store information about you as a user, giving you the ability to return to a site without having to log in again if credentials are required. These cookies that come directly from the website you’re using are called 2<sup>nd</sup> party cookies. 3<sup>rd</sup> party cookies on the other hand are cookies that are installed by vendors other than the website you’re connecting to. 3<sup>rd</sup> party companies, like google or amazon, sell analysis tools that companies can install on their websites that can be used to do this type of tracking. As you visit additional websites, if they are also using these 3<sup>rd</sup> party providers (most are), additional information can be collected about what sites you’re visiting and what you’re doing on those sites.

For many websites the standard method of connection is non-secure. This can usually be determined by the beginning of the web address. If it starts with http, the connection is not secure, and any information sent to the site is in what is called “plain text” and easily readable by anyone who happens to be able to insert themselves between you and the website. DuckDuckGo requires an encrypted connection, denoted by https (the s stands for secure), if available.

DuckDuckGo also provides a privacy “grade” of A-F that is a combination of elements such as the number of hidden tracker networks that were blocked and an evaluation of the website’s privacy policy.

#### Additional Options

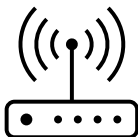


**1. Require a password** or facial recognition to unlock your device. If your phone does not have a password of some type to unlock it, anyone who can gain access to your phone has access to all the data and accounts on your device.


**iPhone:** Go to settings -> Face ID/Touch ID & Passcode

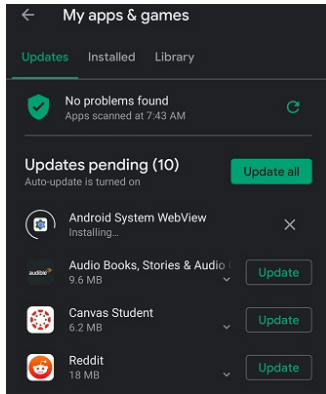
**Android:** Go to settings -> security/biometrics and security -> screen lock

**2. Limit or don't use public WiFi.** Don't allow your device to automatically connect to untrusted networks. Information sent over public WiFi is not secure. That means anything you send over this type of connection is easily intercepted.



In the settings area of your device look for WiFi or Wireless Settings options.

 Any network in range that does not show a locked padlock is not a secure network. Use extreme caution on these types of networks and make sure any checkbox or indicator to automatically reconnect is turned off.

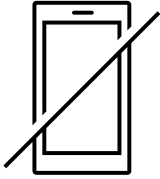


**3. Keep your software up to date.** Many updates to applications are due to discovered security problems that if not corrected could put your private information in danger.

**iPhone:** Visit the app store -> click updates and update all.

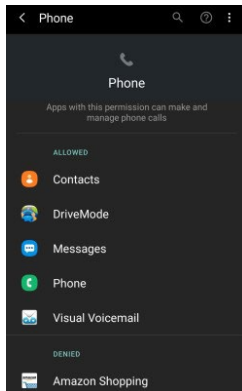
**Android:** Open the Play Store application. From the menu -> my apps & games-> update all.

**4. Set up remote wipe capabilities on your device.** If your device is lost or stolen and you don't have a chance of recovery, this provides a way to remotely delete all the data stored on your device so no one else can access it.



**iPhone:** You will need to set up iCloud and turn on Find My iPhone/iPad on your device. You will sign in with your Apple ID. Once this is turned on, you can access the functions to wipe your device back to factory settings with all data removed.

**Android:** Turn on Find My Mobile in your settings/security section. Once this is available, you will need to log into your provider account: google ([android.com/find](https://android.com/find)), Samsung ([findmymobile.samsung.com](https://findmymobile.samsung.com)), etc. to access features to delete data from your device.



**5. Stop and think about application permissions** when installing applications. We all tend to get in a hurry when installing applications. Take a couple of minutes to really review the permissions that new app is asking for. Are those access abilities really necessary? Are the benefits you're going to get from the application worth giving up that information on you or your friends?

**6. Review installed application permissions.** On a regular basis take a couple of minutes to review the permissions you've granted to applications already on your device. It may be that policies and access have changed since you originally installed it or maybe you don't want to provide the same access.

**iPhone:** Choose settings->privacy. This lists all the permissions available on your phone. You can click on individual permissions to see what applications have that permission. You can disable if you like. For some permissions there are different settings. For location services you may be able to set it to only allow access to your location when the application is being used. Scrolling down far enough will allow you to do the same thing on a per application basis instead of an individual permission.

**Android:** Choose settings-> apps and notifications -> permissions. (there may be differences based on the device provider e.g. Samsung is settings -> privacy). To change a setting select the permission and choose which applications should or shouldn't have access.



**7. Delete apps that you don't use anymore.** Along with reviewing permissions frequently, also review the applications on your phone and if you still use them. There's no reason to provide any type of access to a service you don't use. This also helps clean up storage space on your device and allows you to have sufficient room for those services you do use.

**Appendix B. Survey Instrument**

Construct	Definition	Item	Proposed Measure	Adapted From
Privacy Awareness (7-point Likert)	The extent to which an individual has personal experience with or is aware of the misuse of their data or of the potential for privacy abuse	PA1	How often have you personally experienced incidents whereby your personal information was used by some company or ecommerce web site without your authorization?	Benamati et al., (2017)
		PA2	How much have you heard or read during the last year about the use and potential misuse of the information collected from the internet?	
		PA3	How often has the topic of information privacy been in the news?	
		PA4	How often have you personally been the victim of what you felt was improper invasion of privacy	
Perceived Control of Personal Information (7-point Likert)	The extent to which an individual believes they have control over the management of their personal information	PC1	How much control do you feel you have over your personal information that has been released?	Xu et al., (2012)
		PC2	How much control do you feel you have over the amount of your personal information collected by mobile devices?	
		PC3	Overall, how much in control do you feel you have over your personal information provided/stored on mobile devices?	
		PC4	How much control do you feel you have over how your personal information is being used by mobile devices?	
MUIPC				
Perceived Surveillance (7-Point Likert)	The degree to which an individual believes mobile applications/vendors are continually monitoring user behavior through their mobile devices	PS1	I believe that the location of my mobile device is monitored at least part of the time.	Xu et al., (2012)
		PS2	I am concerned that mobile devices are collecting too much information about me.	
		AC1	Please choose strongly disagree on this question.	
		PS3	I am concerned that mobile apps may monitor my activities on my mobile device.	
Perceived Intrusion (7-point Likert)	The degree to which an individual believes their information personal space or personal boundaries are violated by applications on their mobile devices	PI1	I feel that as a result of my using mobile devices, others know about me more than I am comfortable with.	Xu et al., (2012)
		PI2	I believe that as a result of my using mobile devices, information about me that I consider private is now more readily available to others than I would want.	
		PI3	I feel that as a result of my using mobile devices, information about me is out there that, if used, will invade my privacy	
Secondary use of personal information (7-point Likert)	The degree to which an individual believes their information is shared with other parties outside their control or authorization by applications on their mobile devices	SU1	I am concerned that using mobile devices may allow my personal information to be used for other purposes without notifying me or getting my authorization.	Xu et al., (2012)
		SU2	When I give personal information to use mobile apps, I am concerned that apps may use my information for other purposes.	
		SU3	I am concerned that mobile devices may share my personal information with other entities without getting my authorization.	
Social Influence (7-point Likert)	The extent to which an individual is motivated to	SI1	People who are important to me think that I should be concerned about privacy on mobile devices	Venkatesh et al., (2012)

	act based on their social interactions	SI2	People who influence my behavior think that I should use privacy protection behavior on mobile devices	
		SI3	People whose opinions that I value prefer that I use privacy protection behavior on mobile devices	
Trust (7-point Likert)	The extent to which an individual believes a mobile application/vendor will handle personal data appropriately	TR1	Mobile devices are safe environments in which to exchange information with others.	Dinev and Hart (2006)
		TR2	Mobile devices are reliable environments in which to conduct business transactions.	
		TR3	Mobile devices handle personal information in a competent fashion.	
Habit (7-point Likert)	"The extent to which people have the tendency to perform behaviors automatically" (Limayem et al. 2007 p.705)	HA1	Using mobile device privacy enhancing behaviors has become automatic to me	Limayem et al., (2007)
		AC2	Please choose strongly disagree on this question	
		HA2	Using mobile device privacy enhancing behaviors is natural to me	
		HA3	Using mobile device privacy enhancing behaviors is an obvious choice for me	
Intention to use DuckDuckGo (7-point Likert)	The extent to which an individual plans to use DuckDuckGo, an anti-tracking browser, on their mobile devices.	IU1	I intend to use DuckDuckGo in the next 3 months	Venkatesh et al., (2003)
		IU2	I predict I would use DuckDuckGo in the next 3 months	
		IU3	I plan to use DuckDuckGo in the next 3 months	
Use of DuckDuckGo	The extent to which an individual uses DuckDuckGo as their browser on their mobile devices	UD1	I use DuckDuckGo (7-point Likert)	Venkatesh and Bala (2008)
		UD2	How many times daily do you use DuckDuckGo?	
Controls		CO1	How old are you (in years)?	
		CO2	What is your gender?	
		CO3	What is your academic status?	
Course Credit Information		CC1	Your first name	
		CC2	Your last name	
		CC3	Course number in which you are receiving credit	
		CC4	Your instructor's name	

Appendix C. Tables

	CR	CA	AVE	Hab	Int	PC	PI	PS	PA	SU	SI	Tr
Hab	0.90	0.90	0.75	<b>0.87</b>								
Int	0.99	0.98	0.96	0.15	<b>0.98</b>							
PC	0.90	0.86	0.70	0.15	-0.15	<b>0.84</b>						
PI	0.90	0.84	0.76	-0.06	0.23	-0.26	<b>0.87</b>					
PS	0.89	0.75	0.80	-0.06	0.33	-0.33	0.68	<b>0.90</b>				
PA	0.83	0.62	0.71	0.04	0.27	-0.27	0.42	0.35	<b>0.84</b>			
SU	0.88	0.80	0.72	0.01	0.21	-0.35	0.68	0.73	0.46	<b>0.85</b>		
SI	0.91	0.86	0.78	0.04	0.03	-0.06	0.17	0.11	0.00	0.21	<b>0.88</b>	
Tr	0.85	0.74	0.66	0.00	-0.19	0.26	-0.49	-0.39	-0.20	-0.37	-0.10	<b>0.81</b>

Square roots of AVE shown on diagonal. CR, composite reliability; CA, Cronbach's alpha; AVE, average variance extracted; Hab, Habit; Int, Intention; Int, Intention to Use; PC, Privacy Control; PI, Perceived Intrusion; PS, Perceived Surveillance; PA, Privacy Awareness; SU, Secondary Use; SI, Social Influence; Tr, Trust

Table C-1. Pre-Intervention Survey Question Measures

	CR	CA	AVE	Hab	PC	PI	PS	PA	SU	SI	Tr	Use
Hab	0.95	0.92	0.86	<b>0.93</b>								
PC	0.92	0.88	0.73	0.07	<b>0.85</b>							
PI	0.90	0.82	0.74	0.18	-0.25	<b>0.86</b>						
PS	0.90	0.78	0.82	-0.06	-0.27	0.55	<b>0.91</b>					
PA	0.87	0.70	0.77	0.29	-0.19	0.26	0.32	<b>0.88</b>				
SU	0.92	0.88	0.80	0.16	-0.26	0.63	0.59	0.39	<b>0.90</b>			
SI	0.95	0.92	0.86	0.32	-0.01	0.34	0.34	0.23	0.36	<b>0.93</b>		
TR	0.89	0.81	0.73	0.05	0.29	-0.41	-0.40	-0.17	-0.33	-0.13	<b>0.85</b>	
Use	0.98	0.95	0.96	0.28	0.09	0.15	0.12	0.14	0.25	0.05	-0.09	<b>0.98</b>

Square roots of AVE shown on diagonal. CR, composite reliability; CA, Cronbach's alpha; AVE, average variance extracted; Hab, Habit; Int, Intention; PC, Privacy Control; PI, Perceived Intrusion; PS, Perceived Surveillance; PA, Privacy Awareness; SU, Secondary Use; SI, Social Influence; Tr, Trust

Table C-2. Post-Intervention Survey Quality Measures

	Pre-intervention		Post-intervention	
Stage 1. Dimensions of MUIPC				
	MUIPC		MUIPC	
Perceived Intrusion	2.433		1.935	
Perceived Surveillance	2.549		1.811	
Secondary Use	2.759		2.1	
Stage 2. Latent variable test				
	MUIPC	Intent to use	MUIPC	Use
Perceived Control	1.138		1.124	
Privacy Awareness	1.104		1.104	
Social Influence	1.013		1.07	
Trust	1.106		1.124	
Habit		1.001		1.019
MUIPC		1.001		1.019

Table C-3. Full Variable Collinearity Test

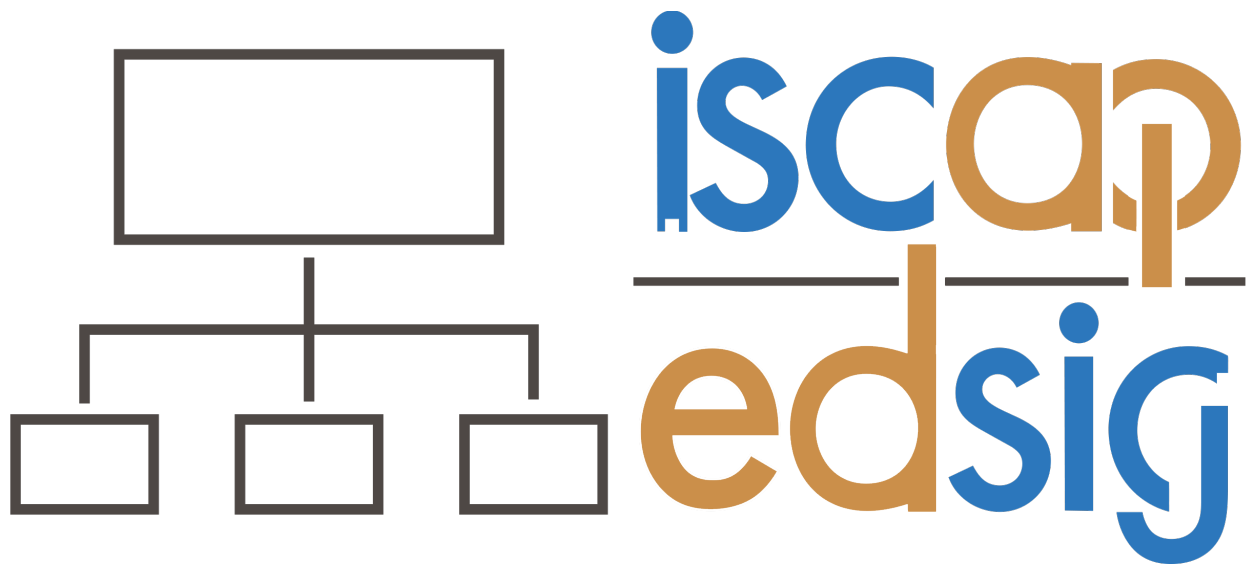
Construct	Indicator	Pre-intervention	Post-intervention	p-value	Significance
		Mean		Paired Differences	
Privacy Experience	PA1	3.24	3.568	0.042	Yes
	PA4	2.808	3.264	0.000	Yes
Social Influence	SI1	4.552	4.76	0.168	No
	SI2	4.408	4.808	0.004	Yes
	SI3	4.768	5.024	0.080	No
Trust	TR1	3.688	3.752	0.649	No
	TR2	3.768	3.912	0.297	No
	TR3	3.92	3.888	0.813	No
Perceived Control	PC1	3.016	3.344	0.019	Yes
	PC2	2.744	3.216	0.000	Yes
	PC3	3.144	3.56	0.001	Yes
	PC4	2.888	3.24	0.008	Yes
MUIPC					
Perceived Surveillance	PS2	5.4	5.208	0.139	No
	PS3	5.288	5.192	0.454	No
Perceived Intrusion	PI1	4.808	4.752	0.643	No
	PI2	5.072	5.016	0.605	No
	PI3	4.832	4.912	0.490	No
Secondary Use	SU1	5.328	5.168	0.145	No
	SU2	5.216	5.216	1.000	No
	SU3	5.44	5.224	0.090	No

Table C-4. Paired Sample T-Tests

	Model 1. Pre-intervention Survey			Model 2. Post-intervention Survey		
	R <sup>2</sup>	Path Coefficient	f <sup>2</sup>	R <sup>2</sup>	Path Coefficient	f <sup>2</sup>
Mobile User's Information Privacy Concern (MUIPC)	0.405			0.394		
Privacy Awareness		0.357***	0.193		0.224**	0.075
Social Influence		0.141**	0.033		0.311***	0.149
Trust		-0.341***	0.177		-0.307***	0.138
Perceived Control		-0.151	0.034		-0.167	0.041
Intent to Use	0.104					
Habit		0.159	0.028			
MUIPC		0.288**	0.092			
Use				0.11		
Habit					0.257***	0.073
MUIPC					0.179**	0.035

\*\*\* p < .001; \*\* p < .05. f<sup>2</sup> ≥ 0.02 = small effect, f<sup>2</sup> ≥ 0.15 = medium effect, f<sup>2</sup> ≥ 0.35 = large effect (Cohen, 1988).

Table C-5. Path Coefficients and Effect Sizes



**Information Systems & Computing Academic Professionals  
Education Special Interest Group**

**STATEMENT OF PEER REVIEW INTEGRITY**

All papers published in the *Journal of Information Systems Education* have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

Copyright ©2023 by the Information Systems & Computing Academic Professionals, Inc. (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to the Editor-in-Chief, *Journal of Information Systems Education*, [editor@jise.org](mailto:editor@jise.org).

ISSN: 2574-3872 (Online) 1055-3096 (Print)