International Journal of Marketing and Business Communication
9 (1 & 2) 2020, 22-29
http://publishingindia.com/ijmbc/

The Role of Privacy in Smartphone Apps Usage

Stephen L. Baglione*, Louis A. Tucci**

Abstract

We studied the importance of online privacy of personal data and security on smartphone apps among undergraduate students. In latent class regression analysis, our independent variables were gender, app usage, and knowledge. A two-cluster solution found evidence of the privacy paradox. Privacy was important, but they spent significant time in location-based apps, which gather data about them and erode their privacy. In both clusters, knowledge, as measured through studying, positively related to privacy concerns. Surprisingly, gender was not statistically significant.

Keywords: Online Privacy Latent Class Regression, Smartphone Apps

Introduction

Malicious apps track user's location, record phone calls, or gather data surreptitiously from your phone. Probably more common is legitimate apps exploiting user's data after users provide permission knowingly or not. Users must balance disclosure and participation online. Many apps are free because business models revolve around selling users' data. Users pay with their data. When downloading, users agree to allow the app to access information on the user's phone (Gu et al., 2017). Information may include contact lists, browsing and search history, calendar, files, photos, networking patterns, location, and time (Egelman, Fit & Wagner, 2013; Pentina, Zhang, Bata & Chen, 2016; Zhou, 2013). Marketers use the information to improve targeting, customer service, and customer relationships (Pentina, Zhang, Bata & Chen, 2016). They also sell the data. Americans are uncomfortable with brands buying and selling their data. Data breaches may occur.

Seven in 10 American cellphone users think advertisers track most of what they do online (Auxier et al., 2019). Almost 70% of Americans believe firms use their data in ways that make them uncomfortable (Auxier et al., 2019). Nine in 10 believe we have lost control of how companies use our data (Pew Research Center, 2014). Yet, apps are extremely popular. The Google Play Store has 2.87 million apps (Statista.com 2020a). In March 2020, the most popular U.S. Android downloaded app was Amazon Shopping with 656,543 (Statista.com 2020b). This disconnect is referred to as the privacy paradox. If true, it would encourage companies to increase users' data collection (Kokolakis, 2017).

Literature Review

Apps

Apps are evaluated on popularity, price, and usability (Kelley, Cranor & Sadeh, 2013; Kim, Park & Oh, 2008). The reasons users download apps are pleasure, saving time, social adjustment, and social pressure (Hui, Tan & Goh, 2006). The dilemma for those downloading the free option: download and accept privacy terms or refuse and be denied access. The privacy terms are immutable (Wottrich, van Reijmersdal & Smit, 2018). Among smartphone app users, 90% believe knowing how their data is used influences their decision to download an app, and 46% uninstalled an app when realizing what information about them was gathered (Olmstead & Atkinson, 2015). About 20% disable a phone's location tracking and a third delete browsing and search data (Boyles, Smith &

* Professor of Marketing and Quantitative Methods, Saint Leo University, United States.
Email: stephen.baglione@saintleo.edu
** Associate Professor of Marketing & Interdisciplinary Business, The College of New Jersey, United States.
Email: ltucci@tcnj.edu

Madden, 2012). Data from health and fitness apps contain health and lifestyle information and geo-location, making it extremely sensitive (Privacy Right Clearinghouse, 2013). "App users are more likely to engage in protection behavior if they feel vulnerable, concerned, and think that they are able to protect themselves from the data collection and usage practices of apps" (Wottrich, van Reijmersdal & Smit, 2019, p. 1074). Highly-valued apps are downloaded regardless of their intrusiveness, while intrusiveness determines whether low-valued apps are downloaded (Wottrich, van Reijmersdal & Smit, 2018).

Privacy Paradox

Westin (1968) defined privacy as "when, how, and to what extent information about them is communicated to others" (p. 7). Warren and Brandeis (1890) offer a more pragmatic definition: It is the right to be left alone. Using these definitions, consumers consistently value privacy, but their actions are incongruent with their values (Acquisti, 2004; Barnes, 2006; Marwick & Boyd, 2014). This incongruence is the privacy paradox, and many have hypothesized its cause.

Downloading an app may offer instant pleasure, while costs may be in the future or nebulous (Acquisti et al., 2016). This is the immediate gratification bias (Acquisti, 2004). Benefit immediacy and risk diffusion contribute (Wilson & Walacich, 2012). Instant benefits also result in higher perceived rewards and lower risks. This relates to hyperbolic discounts: Current benefits are more valuable than future benefits, which are discounted (Acquisti & Grossklags, 2005). Future intentions may be affected by privacy concerns, not actual behavior (Hallam & Zanella, 2017). We believe privacy violations will happen to others, not us (optimism bias) (Baeck, Kim & Bae, 2014; Cho, Lee & Chung., 2014). This relates to how risk is assessed. It is underestimated for items we like and overestimated for items we dislike (Slovic, Finucane, Peters & MacGregor, 2002). We are overconfident in our knowledge and skills. Less than a quarter of those professing knowledge about privacy-enhancing technologies were objectively knowledgeable (Jensen, Potts & Jensen, 2005). Decision-making biases make us irrational (Acquisti, 2004).

Tradeoffs between privacy loss and potential disclosure gain is referred to as the privacy calculus theory (Jiang, Heng & Choi, 2013). In trading off, we seek maximum gains and minimal losses (Li, 2012). Benefits should exceed losses (Sheng, Nah & Siau, 2008). When they do, we provide our data (Lee & Kwon, 2015). In a literature review article (Gerber, Gerber & Vokamer, 2018), strong evidence for privacy calculus was found. This theory has been applied to app use (Fife & Orjuela, 2012; Pentina, Zhang, Bata & Chen, 2016). Among tech-savvy users, functionality and design were shown experimentally to outweigh privacy concerns (Barth et al., 2019).

Mobile computing decision-making may be irrational because decisions are context-dependent and happen fast and on-the-go (Barth & de Jong, 2017). Hoffmann, Lutz, and Ranzini (2016) suggest that privacy cynicism serves as a coping mechanism for dealing with overwhelming threats to privacy. Privacy is neglected by many users because it is viewed as hopeless. Understanding privacy policies may require a level of technical expertise (Hargittai, 2009). Baek (2014) supports this by showing how counter-arguments or providing both sides of an argument influence respondents, indicating online privacy attitudes lack a foundation. A meta-analysis of the privacy paradox found the discrepancy was not as pronounced as earlier thought (Baruh, Secinti & Zeynep, 2017).

Hypotheses

If the privacy paradox exists, clusters should manifest based upon online privacy and app usage rates. Into this mix, we add gender, and knowledge through a proxy, hours spent studying. The population is undergraduate college students. Prior research indicates this group (18 to 24 years of age) has the highest daily mobile app usage at 3.2 hours (Blair, 2020). Respondents were primed by telling them that apps use their personal information. Priming has been shown to influence app selection (Rajivan & Camp, 2016). Privacy concerns are affected by usage rate (Tsay-Vogel, Shanahan & Signorielli, 2018). For heavy users, risk perception increased longitudinally, while they were steady for light users. When examining benefits and risks in location-based social network services such as Facebook, males rely on benefits and females on risks (Sun, Wang, Shen & Zhang, 2015). Women are more concerned about privacy in shared Facebook pictures (Malik, Hiekkanen & Nieminen, 2016). Among demographic variables in a literature review, only gender predicted privacy behavior, with women having higher concern levels (Gerber, Gerber

& Volkamer, 2018). Knowledgeable users of mobile apps displayed less protection motivation and behavior (Wottrich, van Reijmersdal & Smit, 2019). This study used hours spent studying as a proxy for knowledge. The model is online privacy is a function of app usage, gender, and knowledge. Our hypothesis are:

H1: Clusters will exist for the dependent variable: involvement with online privacy of data and security based upon app usage, gender, and knowledge.

H2: At least one cluster will exhibit the privacy paradox. Involvement and app usage rate will be high.

H3: Clusters will differ on online privacy based on gender, with females having higher concerns.

H4: Clusters will differ on online privacy based on knowledge, with more knowledge leading to lower concerns.

Methodology

Differences among the variables of our hypotheses are examined through clusters. To determine whether clusters exist we used latent class regression analysis (Wedel & Kamakura, 2000). Latent-class regression was used to determine if the sample was homogenous or contained distinct clusters. The BIC and AIC also measure parsimony by adjusting the L^2 based on model parameters estimated. To assess model fit, the likelihood-ratio goodness-of-fit value (L^2), BIC, and AIC were estimated (Vermunt & Magidson, 2005). Lower values for all three are preferable. Finally, respondents are assigned to clusters based on highest membership probability. Misclassification error rates close to zero are best. Using the mean squared error, an R^2 is estimated (Vermunt & Magidson, 2005).

The dependent variable is a previously validated scale on involvement (Zaichkowsky, 1994). It is an eight-item seven-point scale. The question is online privacy of your data and security followed by bi-polar adjectives (e.g., important/unimportant; means a lot to me/means little to me; beneficial/not beneficial; essential/non-essential; wanted/unwanted; useful/useless; and valuable/worthless). Two items are negatively worded and were reverse coded before analysis. Internal consistency is estimated through coefficient alpha (Fornell & Larcker, 1981). If internally consistent, the scale items will be summed.

Results

The survey was pretested using protocol analysis in a graduate marketing research class. Students conducted the pretest on people outside the class. Each student completed four pretests (total of 12), and modifications were made to the survey. A convenience sample of students from six traditional-aged undergraduate business classes at a southeastern university were asked to complete the survey in Qualtrics. They were emailed a link and promised anonymity and confidentiality Those who do not use location-based apps were excluded.

Eight students started but did not complete the survey and were removed from the analysis. One-hundred-and-twenty-six students completed the survey. Three students had very low variability among the Likert-type questions. An examination of their responses indicated neutrality about privacy; however, other questions were answered with diligence. These observations were retained. For outliers, Mahalanobis Distance was estimated where the dependent variable is respondent number and the independent variable those used in the analysis (Tabachnick & Fidell, 2013). Multivariate outliers are unaffected by the dependent variable in a regression. Two observations were removed because they exceeded the critical values of a chi-square test. No question had missing values. Three observations were removed because their influence (Cook's distance) was greater than one (Tabachnick & Fidell, 2013). (Note: Unlike Cook's distance, Mahalanobis is not unique to regression).

The sample is overwhelmingly female (65%) and business majors (90%). Almost 80% are sophomore (31%) or juniors (48%). They are predominately from suburban areas (63%), followed by rural (19%) and urban (18%). Almost one in five students (19%) does not belong to a student organization. The average is almost two, which includes those who do not participate. One third are student-athletes.

From Monday to Friday, students spent an average of 12 hours on apps (range from two to 28) and 10 hours on weekends (range from one to 28). They worked an average of eight hours in the past seven days (range from zero to 61). (Note: This was distributed during the COVID 19 pandemic.) They studied over 21 hours in the past week (range from one to 80). The average GPA is

3.26 (range of two to 4.00), and the average age is 20.5 (range 18 to 29).

Table 1: Demographics (n=121)

Attribute	*Level*	*Percentage*
Gender [1]		
	Female	65
	Male	36
Major		
	Business	90
	Non-business	10
Class Rank		
	Freshman	9
	Sophomore	31
	Junior	48
	Senior	11
Residence		
	Rural	19
	Suburban	63
	Urban	18

[1] Because of rounding error may not sum to 100

Latent class regression was estimated, with the dependent variables being the involvement scale for online privacy. Coefficient Alpha for the eight-items is .829, indicating acceptable internal consistency. This exceeds the threshold for scale reliability (i.e., internal consistency) of 0.70 (Fornell & Larcker, 1981).

The Log-likelihood declines from the two to five clusters (Table 2). The BIC increases slightly from two to five clusters; the difference between two and three clusters is negligible. The AIC fluctuates, decreasing from two to three, then increasing from three to five. The classification error is 5% with two clusters, doubles with three, and doubles again with four (25%). The two-cluster model is most appropriate, given the statistics and parsimony. Hypothesis one is supported.

Table 2: Cluster Comparison (n=121)

Statistic/Clusters	*Two*	*Three*	*Four*	*Five*
Log-likelihood	-375.18	-361.23	-358.48	-353.70
BIC	803.12	803.98	827.26	846.47
AIC	772.37	756.45	762.95	765.39
Classification Errors	.05	.11	.25	.25

The regression model explains 71% of the variation in the involvement scale measuring online privacy (Table 3). 14% of the variation in the first cluster and 80% of the second are explained. With a scale neutral point of 32 (eight items times a midpoint of four), both clusters believe online privacy is important, means a lot, beneficial, wanted, useful, and valuable (below scale neutral point). Among the three independent variables, only gender is not statistically significant. Hypothesis three is not supported.

Cluster One (80%) is four times the size of Cluster Two (20%). Cluster One has a negative relationship (-.04) between app usage weekly and involvement with online privacy. As usage increases, anxiety about online privacy increases (lower values indicate more involvement). This cluster's app usage is almost 23 hours weekly. They are very concerned about online privacy but use apps that may violate it often. This supports Hypothesis Two. The amount of weekly studying also has a negative relationship (-.10) with online privacy. If knowledge is a proxy for studying, the more knowledgeable a user is the more concerned he/she is about online privacy. Cluster Two has a positive relationship with app usage (.16). As app usage increased, privacy concerns decreased, but they were still concerned since their mean (25.29) is below the multi-item scale midpoint. Cluster app usage is almost 21 hours. This partially supports Hypothesis Two. They are concerned about online privacy yet use apps extensively. Their concern diminishes the more they use apps.

Knowledge, as measured through the proxy of hours spent studying, is statistically significant. For both clusters, an increase in studying makes them more concerned about online privacy. Hypothesis Four is supported. Cluster

Table 3: Two-Cluster Solution (n=121)

Variable	*One*	*Two*	*Wald*	*P-Value*	*Overall*
Cluster Size	80%	20%			
R^2	.14	.80			.71
App Usage (weekly)	-.04	.16	14.44	.00073	
Gender (female)	.77	.92	3.51	.17	
Studying (weekly)	-.10	-.27	50.16	1.3e-11	
Privacy Scale (mean)	13.18	25.29			
App Usage (mean)	22.73	20.72			

General Discussion

Both clusters indicated that privacy was important, yet users spent significant time on location-based apps that gather data about them and erode their privacy. These location-based apps, at a minimum, collect data from them to tailor advertisements and, in many cases, gather much more: contact lists, browsing and search history, files, photos, etc. (Egelman, Fit & Wagner, 2013; Pentina, Zhang, Bata & Chen, 2016; Zhou, 2013). There is information there that almost everyone would want private. This exemplifies the privacy paradox (Acquisti, 2004; Barnes, 2006; Marwick & Boyd, 2014). Behavior conflicts with attitudes. Americans, in general, know they are being tracked online by advertisers when they use their smartphone and are concerned about how that data is used (Auxier et al., 2019), but they do it anyway.

Maybe they believe they can "protect themselves from the data collection and usage practices of apps" (Wottrich, van Reijmersdal & Smit, 2019, p. 1074). Why would they still use the apps? Have the apps become indispensable and privacy a quixotic notion? Have smartphone apps become so convenient and ingrained in daily life that no one can envision life without them? If indispensable, the privacy terms are immutable and must be accepted to download the app (Wottrich, van Reijmersdal & Smit, 2018). Users must accept them. Or does immediate gratification override everything else (Acquisti, 2004). Do higher perceived rewards results in lower perceived risk (Wilson & Walacich, 2012)? Regardless, mobile phone decision-making is context-dependent and happens quickly (Barth & de Jong, 2017).

Users also may be trading off between privacy and potential disclosure or the privacy calculus theory (Jiang, Heng, and Choi, 2013). Perceived benefits may outweigh perceived losses (Fife & Orjuela, 2012; Gerber, Gerber & Vokamer, 2018; Pentina, Zhang, Bata & Chen, 2016; Sheng et al., 2008). One cluster's privacy concerns increase with app usage while the other decreases. Is privacy cynicism occurring where users see protecting privacy as hopeless (Hoffmann, Lutz & Ranzini, 2016)? When you use apps more, do you give up trying to maintain your privacy? Knowledge tempers privacy concerns. More knowledgeable users have greater concerns about online privacy. Prior research indicated risk perceptions increased with usage (Tsay-Vogel, Shanahan, and Signorielli, 2018); however, our research did not classify what heavy and light users.

Is education or a counter-argument the answer (Baek, 2014)? Knowledge alone does not stop marketers from imposing their will with data privacy by forcing respondents to accept privacy terms to use the app. The implications for marketing are users are not concerned enough to stop using valuable mobile apps (Kokolakis, 2017). The privacy paradox allows them to maintain current business practices. Regulation seems the only option for change.

Surprisingly, gender differences on privacy were not found; women were not more concerned with privacy than men, which contradicts prior research (Malik, Hiekkanen & Nieminen, 2016; Sun, Wang, Shen & Zhang, 2015). Knowledge indicates greater concern for online privacy. This contradicts prior research where more knowledgeable mobile app users were speculated to have given up trying to protect themselves because of the difficulty (Wottrich, van Reijmersdal & Smit, 2019).

Future Research and Limitations

Respondents indicated they use location-based apps and self-reported usage rate; we did not independently verify it. Our sample was more female than male. Generalizability is limited since a convenience sample was utilized. Privacy breaches are relatively rare, and self-reported behaviors for infrequent events are unreliable (Staddon, Acquisti & Lefevre, 2013). Involvement of online privacy is influenced by the fact that data breaches are rare.

Future research should construct clusters that explain why app users express concern for privacy but disregard it with location-based apps. These theories include: third-person theory, optimism bias, objective knowledge, hyperbolic discounting, privacy calculus, communication privacy boundary management, and dispositional privacy concerns (Acquisti & Grossklags, 2005; Baeck, Kim & Bae, 2014; Choi, Wu, Yu & Land, 2018; Debatin et al., 2009; Jensen, Potts, and Jensen, 2005; Jiang, Heng & Choi, 2013; Petronio, 1991; Slovic et al., 2002). Respondents should be asked whether they believe online privacy is under their control and how important location-based apps are in their lives.

Have users disabled their phone's location tracking or deleted browsing and search history (Boyles, Smith & Madden, 2012)? This could be included in future clustering research to determine its impact on online privacy. Health and fitness apps are flourishing commercially and collecting extremely sensitive data. These users could be studied (Privacy-Right Clearinghouse, 2013).

Using experimentation, we could manipulate an app's popularity and price since they influence downloading (Kelley, Cranor & Sadeh, 2013; Kim, Park & Oh, 2008; Wottrich, van Reijmersdal & Smit, 2018). Levels for the experiment would be a free version with tracking and a premium version without. The second variable would be the popularity of the app (high or low).

References

Acquisti, A. (2004). *Privacy in electronic commerce and the economics of immediate gratification.* ACM Conference on Electronic Commerce, New York.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy*, *2,* 24-30.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and privacy: Concerned, confused and feeling lack of control over their personal information, *Pew Research Center*, November 15. Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Baek, Y. M. (2014). Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behavior, 38,* 33-42.

Susanne 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,* 1038-1058.

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday,* 11(9). Retrieved from https://firstmonday.org/ojs/index.php/fm/issue/view/203

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41,* 55-69.

Baruh, L., Secinti, E. & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review, *Journal of Communication*, *67,* 26-53.

Blair, I. (2020). Mobile app download and usage statistics. Retrieved from https://buildfire.com/app-statistics/

Boyles, J. L., Smith, A., & Madden, M. (2012). Privacy and data management on mobile devices. Retrieved from http://www.privacylives.com/wp-content/uploads/2012/09/PIP_MobilePrivacyManagement-092012.pdf

Cho, H., Lee, J. S., & Chung S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987-995.

Debatin, B., Lovejoy J. P., Horn A. K., & Hughes B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83-108.

Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy: There's a price for that. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 211-236). Heidelberg: Springer.

Fife, E., & Orjuela, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management*, *4*(11), 1-10.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50.

Gerber, N., Gerver, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77,* 226-261.

Gu, J., Xu, Y., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94,* 19-28.

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior, 68,* 217-227.

Hargittai, E. (2009). An update on survey measures of web-oriented digital literacy. *Social Science Computer Review*, *27*(1), 130-137.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Journal of Psychosocial Research on Cyberspace*, *10*(4).

Hui, K.-L., Tan, B. C. Y., & Goh, C.-Y. (2006). Online information disclosure: Motivators and measurements. *ACM Transactions on Internet Technology (TOIT)*, *6*(4), 415-441.

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), 203-227.

Jiang, Z., Heng, C. S., & Choi, B. C. F. (2013). Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, *24*(3), 579-595.

Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013). Privacy as part of the app decision-making process. *CHI Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 11.

Kim, G. S., Park, S.-B., & Oh, J. (2008). An examination of factors influencing consumer adoption of short message service (SMS). *Psychology & Marketing*, *25*(8), 769-786.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computer & Security*, *64,* 122-134.

Lee, N., & Kwon, O. (2015). A privacy-aware feature selection method for solving the personalization-privacy paradox in mobile wellness healthcare services. *Expert Systems with Applications*, *42*(5), 2764-2771.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471-481.

Malik, A., Hiekkanen, K., & Nieminen, M. (2016). Privacy and trust in Facebook photo sharing: Age and gender differences. *Program Electronic Library and information Systems*, *50*(4), 462-480.

Marwick, A., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051-1067.

Olmstead, K., & Atkinson, M. (2015). Apps permissions in the Google Play store. In Pew Research Center, October. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/interactives/apps-permissions/

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, *65,* 409-419.

Pew Research Center. (2014). Public perceptions of privacy and security in the post-snowden era. Retrieved from http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

Privacy Right Clearinghouse. (2013). Mobile health and fitness apps: What are the privacy risks? Retrieved from https://www.privacyrights.org/mobile-health-and-fitness-appswhat-are-privacy-risks

Rajivan, P., & Camp, L. J. (2016). Influence of privacy attitude and privacy cue framing on Android app choices, Symposium on Usable Privacy and Security (SOUPS), Denver, Colorado.

Sheng, H., Nah, F. F.-H., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems*, *9*(6), 15.

Slovic, P., Finucane, M., Peters, E., & MacGregor, D. G. (2002). The affect heuristic: The psychology of intuitive judgment. In: T. Gilovich, & D. Kahneman (Eds.), *Heuristics and Biases* (pp. 397-420), Cambridge, United Kingdom: Cambridge University Press.

Staddon, J., Acquisti, A., & LeFevre, K. (2013). Self-reported social network behavior: Accuracy predictors and implications for the privacy paradox. In *Proceedings of the 2013 International Conference on Social Computing.*

Statistica.com (2020). Leading shopping apps in the Google Play Store in the United States in March 2020, by number of downloads. Retrieved from https://www.statista.com/statistics/819732/leading-google-play-shopping-usa-downloads/

Statista.com (2020b). Number of available applications in the Google Play Store from December 2009 to March 2020. Retrieved from https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender difference. *Computers in Human Behavior*, *52,* 278-292.

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (6th ed.). Pearson, Boston.

Tsay-Vogel, M., Shanahan, J., & Signorielli N. (2018). Social media cultivating perceptions of privacy: A

5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media and Society*, *20*(1), 141-161.

Vermunt, J. K., & Magidson, J. (2005). *Latent gold 4.0 user's guide: Statistical innovations inc.* Belmont, Massachusetts.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220.

Wedel, M., & Wagner, K. A. (2000). *Market segmentation: Conceptual and methodological foundations* (2nd ed.). Norwell, MA: Kluwer Academic Publishers.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum, New York: Atheneum Press.

Wilson, D., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. In *Proceedings of the 33rd International Conference on Information Systems,* December 16-19.

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, *106,* 44-52.

Zaichkowsky, J. L. (1985). Measuring the involvement construct. *Journal of Consumer Research*, *12,* 341-352.

Zhou, T. (2013). Examining continuous usage of location-based services from the perspective of perceived justice. *Information Systems Frontiers*, *15,* 141-150.