Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

Post Data Breach Use of Protective Technologies: An Examination of Users' Dilemma

Emmanuel W. Ayaburi
University of Texas RGV
emmanuel.ayaburi@utrg.edu

Francis K. Andoh-Baidoo
University of Texas RGV
francis.andohbaidoo@utrgv.edu

Jae Ung (Jake) Lee
Louisiana Tech University
jakelee@latech.edu

Abstract

This preliminary research addresses the technology use uncertainties that arise when users are presented with protective technologies following a data breach or privacy violation announcement. Prior studies have provided understanding of determinants of technology use through several perspectives. The study complements prior research by arguing that, beyond individual dispositions or technology features, data breach announcements bring users' focus on the actions of the breaching organization. Fair process and information practices provide avenue for organizations to alleviate users' concerns and increase service usage. We draw on organizational justice theory to develop a model that explicates the effect of organizational fairness process and use of technologies. We test this model using data from 200 Facebook users recruited from Amazon MTurk. We found that procedural and informational justice have differential effect on users' desire to use protective technologies. Our findings have both theoretical and practical implications.

1. Introduction

Data breaches, that have caused significant financial and sensitive information loss, continue to threaten individuals' privacy and organizations' critical information infrastructure [36]. Data breaches such as the Marriott International Starwood breach (2018) involving 500 million individuals, or the Facebook/Cambridge Analytica scandal affecting over 50 million user accounts have exacerbated users' concerns about emerging technologies [1, 18]. The trend is not showing a slowing down as over a third (36%) of global organizations were breached in 2017 [25]. Efforts to protect users from further damage usually involve offering protective technologies or services. For example, after the Marriot Hotel reservation system breach, the hotel chain offered its guests fraud-detecting service, a protective technology, aimed at providing security assurance for its client base [28]. In another instant, after the public announcement of the Cambridge Analytica scandal, Facebook planned to offer users a protective technology - "Clear History", that allows users to force Facebook to delete all the information it gathers about them [40]. These countermeasures or actions taken by breached or violating entities may be futile if users do not adopt and use them.

Some researchers have looked at the problem of technology adoption or use from diverse perspectives including technology features, task, organizational or personality traits [15, 32, 38]. These studies have employed theories including technology acceptance model [15], unified theory of acceptance and use of technology [38], innovation diffusion theory [32], and big five personality traits [21]. Prior research has emphasized that the technology's usability, fit with the task at hand or individual's technology disposition are antecedents of technology use. Additionally, the confirmation of users' expectations influences their desire to continuously use the technology [4]. However, when users experience a violation of their privacy, their perceptions of the preceding factors may be negatively influenced. For example, users trust in a technology is eroded or their routine use of the technology is halted when they experience a data breach [26]. In some cases, users provide negative recommendation through electronic word of mouth. Given the potential negative effect of violation on predictors of technology use or adoption, we seek in this study to understand the following research question: post data breach announcement, *what organizational actions influence the likelihood of using protective technologies?*

Explicating the underlying factors that lead individuals to adopt and use protective technologies is thus, the central goal of the current study. To answer the above research problem, we draw on organizational justice theory [11], to develop a model that explicates the effect of organizational fairness process and use of technologies. In this preliminary study, we gather data

URI: https://hdl.handle.net/10125/64262
978-0-9981331-3-3

on key perceptions of clear history tool, an ideal candidate protective technology by Facebook following the Cambridge Analytica data breach, from Facebook users to test our research model. Analysis of survey responses provides insights into the mechanism by which privacy crisis could be managed through the offering of appropriate protective tools. By investigating and understanding the actions of the privacy violating entity, we complement prior studies on protective technology adoption and use. We contribute to the body of knowledge related to breach management, business crisis management and protective technology use by providing insights for research and practice. Overall, this paper offers two contributions to literature. One, our study identifies key dimensions of organizational justice that are relevant determinants of individuals' use of a technology. In doing so, we help identify the actions that positively facilitate post data breach crisis management. Two, our findings show which dimension of organizational justice has greater influence on users' intention to use a protective technology post data breach. Thus, the study identifies the theoretical linkage between organizational justice and technology use during crisis management. Taken together, these outcomes provide insights for managers to optimize their actions to manage users' decision to use protective technology after data breach.

The structure of the rest of this paper is as follows: next is the discussion of literature related to this study, followed by a presentation of the research model development and hypotheses testing, and finally results, discussion of the results and contributions of the study.

2. Background Literature

2.1. Protective Technology Use

Protective technologies are information technologies that monitor or prevent unauthorized access or modification of data [17]. An example of protective technologies is anti-spyware software that protects users' devices from unauthorized access. Prior IS research (see Table 1) have explored factors influencing the adoption of protective technologies through the lens of technology acceptance model, theory of planned behavior and protection motivation theory (PMT). Key predictors of protective technology adoption include the user level of technology awareness [17], coping appraisal [6, 22], users' cultural background [13, 17] and the users' computer self-efficacy [27].

However, new protective technologies are been introduced to further provide users protection when affected by a data breach. One such example is credit monitoring and fraud detection technologies that aim to prevent further abuse of victims of data breaches. As noted by Ng et al., [27], breach experience should affect users' intention to adopt or use protective technologies. Although prior literature has expanded our understanding on the use of these types of technologies, little is known about influencing factors after an announcement of violations. Additionally, little is known about the effect of actions that are implemented by breach/violating organization on victims' intention to use recommended protective technologies. We contend that because the same entity serves as conduit for the data breach and recommender of the protective technology, users' decision may not be entirely based on the technical features of the technology. We explore in this study, how users' perception of the fairness of the action or information provided, key tenets of organizational justice theory, influence their intention to use protective technologies.

Table 1. Summary of some key literature of Protective technology use

Problem	Findings	Reference
What factors that influence intentions to use protective technologies and how do they contribute to the formation of this intention?	Users' technology awareness influences their intention to use protective technologies in pre-data breach context. Major constructs of TAM (ease of use and usefulness) and TPB (subjective norms and control) influence intention to use protective technologies in pre-data breach context.	[17]
Which coping factors influence consumers to adopt various identity protection practices?	Conventional and technological copings are key to individuals handling of identity theft incidence.	[22]
What factors facilitate and/or impede intentions to adopt anti-spyware?	Effort and time instead of monetary cost are key in user's cognitive appraisal. Cognitive appraisal process affects the likelihood of using anti-spyware software, an example of a protective technology	[6]

What is the role of cultural factors in the use of protective information technologies?	A user's cultural background including individualism, masculinity, power distance, and uncertainty avoidance moderates their core tenets of technology adoption factors and intention to use protective technologies. Technology awareness is a stronger predictor of protective technology use in an individualism and masculine cultures	[16]
What is the influence of culture on individual's security behavioral intention?	Users' individualism–collectivism and uncertainty avoidance cultural background affect protection motivations which subsequently influence their intention to use protective technologies.	[13]
What are the salient influences for a user to practice computer security in an organization?	Individuals perceived skills, appraisal of their susceptibility threat and benefits affect their positive computer security behavior Severity of the threat moderates the effects of these factors on user security behavior.	[27]

2.2. Organizational Justice Theory

Organizational justice theory argues that, individuals' perception about the actions of an organization as an entity influence their attitudes and behaviors towards the organization [19]. Such individuals could be within or outside the organization with relationship with the organization. Pertinent to the organizational justice theory is that, fairness is the main link between the actions of the organization and trust in its services. Organizational justice theory consists of three key components – procedural justice, distributive justice and interactional justice [11]. While procedural justice focuses on the fairness and objectiveness of the process that guide decision-making, distributive justice emphasizes the perceived fairness regarding equity or equality of decision outcomes and interpersonal justice focuses on the fairness of the interpersonal treatment accorded all parties involved [19]. The third component, interactional justice, is further decomposed into interpersonal justice and informational justice. Whereas interpersonal justice looks at treatment regarding politeness, dignity and respect, informational justice focuses on the nature of justification and truthfulness regarding information about explanations provided when actions are taken to resolve a conflict [12]. For example, in the context of policy compliance or job performance, organizations exhibit procedural justice by taking actions that seem fair in dealing with employees, show distributive justice by applying just reward without discrimination for compliant employees, and/or demonstrate interaction justice by providing objective and timely information in their interactions with employees regarding policies and procedures [23].

Justice perceptions are important in promoting good citizenship behavior by individuals. In the information systems context, the concept of organizational justice has been used to understand customer concerns and trust. Following a data breach or privacy violation or scandal, breach entities are required by law to provide their users and affected individuals information about the causes of the breach, time of the breach and actions taken to restore users' privacy. The procedures taken or information provided are supposed to help maintain user trust by ensuring that users are treated fairly, and the organization is seen as having behavioral integrity [2, 33]. Breaching entities thus foster procedural justice by providing input into key decisions and/or foster information justice by been ethical and providing affected users truthful information [19]. However, breaching entities usually do not provide rewards to affected individuals nor share the cost of breach with affected users. Sharing of reward or cost are key components of distributive justice [19]. Thus, we employ the concepts of procedural justice and informational justice from the organizational justice theory to understand how they influence the use of protective technologies post data breach.

3. Hypotheses Development

3.1. Procedural Justice

Procedural justice refers to users' perception of the procedures an entity such as Facebook uses to make decisions regarding its fiduciary responsibility to its users [19]. It relates to the fairness of the process employed to evaluate and resolve issues about privacy violation. Procedural justice has been found to influence individuals' behavioral outcomes [39]. Drawing on prior studies, we argue that the level of perceived procedural justice influences the attitudes and beliefs of users about the need to use tools promoted by the violating entity. When users feel the entity, to which they make themselves vulnerable to by entrusting their sensitive information, is acting in good faith, users will accept apologies and subsequently restore their trust in the entity [37]. Indeed, the fairer the violating entity's procedures, the more likely that the user will trust the entity despite the publicity of data breach. Increase in trust has been found to influence users' intention to use technology [3]. Therefore, following data breach publicity, we expect that:

H1: Individuals' perception of the organization's procedural justice is positively related to use of protective technologies.

3.2. Informational Justice

Informational justice refers to perceived openness and trustworthiness of an entity such as Facebook in communicating important issues with its users [19]. Organizations which place premium on informational justice would not only provide clear and sufficient information but will also be transparent about the process and outcome with those affected by their decisions [34]. Information practices during and after an unfortunate incident that address users' risk perception may lead to positive perceptions about trust. Because users may have developed attachment to a service or a product prior to a violation, they may have high switching costs if they consider moving to other services. However, fair information practices provide users some level of control over future information disclosure regarding the breach incident. Thus, a high level of perception of informational justice may affect users' intention by lowering any personal objections against the entity's proposed remedies to the violation. Hence, following data breach publicity, we postulate that:

H2: Individuals' perception of the organization's informational justice is positively related to use of protective technologies.

3.3. Procedural Justice versus Informational Justice

We contend that procedural justice instills the sort of legitimacy needed to motivate users to trust a violating entity. While informational justice provides users with data about how the violating entity proposes to resolve users concerns, it is the fairness of the procedures or action that promotes user's perception of behavioral integrity in the organization [33]. Users' perception of behavioral integrity positively affects their trust in an entity and subsequent intention to use its services or product [3]. We argue that an organization's procedural justice will strongly reduce users' concerns than information justice as users view information without actions as cheap talk [18]. Therefore, following data breach publicity, we expect that:

H3: Procedural justice has greater positive effect than informational justice on individual's likelihood of using protective technologies.

Control Variables: Individuals' privacy concerns affect use of technologies [5]. Reduction in privacy concerns should translate to increase trust in the technologies or platforms [35]. Additionally, prior research has suggested that individuals' age and experience affect their intention to use a technology. Therefore, we control for respondents' general privacy concerns, age and experience.

4. Methodology

4.1. Sample and Study Context (Clear History)

Examples of protective technologies in use by organizations and individuals include anti-virus, antispyware, firewalls, intrusion detection, encryption, decryption and prevention intrusion. These technologies are supposed, among other things, to prevent the violation of users. Following the discovery and subsequent announcement of privacy scandal by Cambridge Analytica of Facebook users, the social media giant postulated that some users may become skeptical about using its services. To alleviate users' concerns and provide assurances of non-repeat of future violation, Facebook has been planning to introduce Clear History Tool (CHT). CHT is a protective technology that provides users the option to ask the social media platform to delete all the information it gathers about them. We expect that the scale and publicity of the breach scandal would affect users' decision to use CHT. There is no known academic study that looks at the use of protective technologies including CHT after a data breach. Thus, CHT provides an ideal context to investigate our research problem with a target population.

The population of interest for this study are users of Facebook before the publicity of the privacy scandal. Respondents are Facebook account holders recruited from Amazon MTurk, which was deemed appropriate since our target respondents have experience of the research context. Participation was limited to users in North America to minimize any confounds unique to users' cultural background. Following [24], we included attention-trap questions such as "George W. Bush is the current president of the US. T/F". We received 200 usable responses. Male (67%) and female (33%) respondents were almost equally represented, and an average age of respondent was 36 years with average 8.3 years of experience using Facebook.

4.2. Measures

Whenever possible, this study used previously validated measures and adapted them in the context of post privacy breach context. The constructs were measured with multiple indicators coded on a five-point Likert scale. Most items for the constructs exhibited desirable psychometric properties. Table 2 shows operational definitions of the constructs used in the study.

Table 2. Constructs operational definitions

Construct	Definition	References
Procedural Justice	The perceived fairness of decision-making processes involving Facebook users as a result of a privacy violation	[11]
Informational Justice	The perceived openness and trustworthiness in communicating with Facebook users as a result of a privacy violation	[23]
Technology Use	Facebook user intention to use a technology that provides cyber protection recommended by Facebook	[17]

4.3. Preliminary Analysis and Results

The testing of our research hypotheses was done using partial least square (PLS) analysis using SmartPLS version 3.2.7 [30]. The choice of a component-based SEM was informed by the robustness of PLS in cases of smaller samples and because of its ability to specify and test path models with several latent constructs. Furthermore, PLS does not necessitate any assumptions of multivariate normality [8, 20]and is suited for complex models with latent variables. In addition, a bootstrap procedure with 5,000 re-samples were used to assess the statistical significance of the loadings and of the path coefficients [30].

As shown in Table 3, the composite reliability (CR) of each construct ranged from 0.73 to 0.92; the average variance extracted (AVE) ranged from 0.55 to 0.77, and most of the item loadings were higher than 0.70. All these measures meet the recommended levels. One item (PC3) of one of the control variables -general privacy concerns- was dropped because of poor loading (0.2). All other items with decent loadings of approximately 0.6 were maintained, as this is a preliminary exploratory study (see appendix). All other factor loadings were above 0.70 demonstrating convergent validity or above [7]. Discriminant validity of each latent construct was tested using the heterotrait-monotrait (HTMT) ratio of correlation method recommended by Hair et al. [20]. It is suggested that, discriminant validity issues exist when HTMT values are high. A threshold value of 0.85 is recommended. This criterion is satisfied by all latent constructs.

Table 3. Reliability, AVE and HTMT ratios

Con.	**CR**	**rho_A**	**AVE**	**PJ**	**IJ**
PJ	0.73	0.76	0.55		
IJ	0.92	0.92	0.74	0.79	
LK	0.85	0.85	0.77	0.50	0.34

Note: Off-diagonal elements are HTMT ratios

We conducted model robustness checks for multicollinearity by performing a variance inflation factor (VIF) test. Individual VIF values were as follows: procedural justice (1.74) and informational (1.82); these values were at satisfactory levels (VIF < 5), indicating multicollinearity was not a serious threat to the robustness of our results.

Common method bias is considered an issue when one single factor accounts for the majority of the covariance among the variables [29]. Harman's single factor test was conducted to estimate if the effect of common method variance (CMV), which is a function of the methods employed to measure the independent and dependent variables, was a threat to the validity of the study results [29]. All items were loaded onto a single factor in an exploratory factor analysis without rotation. The test showed that the factor that accounted for largest variance extracted is 33.79%, providing evidence that common method bias was not a threat to the study. The preceding results demonstrate that our measurement model exhibits sound psychometric properties that is necessary for further testing of the research hypotheses.

4.4. Results of Hypothesis Tests

Component-based partial least squares (PLS) analysis was used to test the structural paths proposed in this study. PLS is appropriate for prediction, exploration and theory development. From our test results, our model explains approximately 20.6% of the variance in post data breach protective technology use. In support of Hypothesis 1, procedural justice was found to have a significant positive impact on likelihood of using protective technology such as CHT (b = 0.303, t= 3.73, p<0.05). Hypothesis 2 states that, informational justice is positively related to likelihood of using protective technology such as CHT. This hypothesis was supported (b = 0.182, t=2.124, p < 0.05). To test H3, we followed the path coefficient comparison method proposed by [10] using the equation below:

$$t = \frac{\beta 1 - \beta 2}{\sqrt{(SE\beta 1)^2 - (SE\beta 2)^2}}$$

$where$ SEβ is the standard error of β

We did find significant differences between the effects of procedural justice or informational justice on desire use CHT (*b* = 0.121, *t*= 4.40, *p*<0.05). For our control variables we did not find support for age (*b* = 0.025, *t*= 0.407, *p*>0.05) nor experience using Facebook (*b* = 0.082, *t*= 1.099, *p*>0.05). However, we did find marginal support for users' general privacy concerns (*b* = 0.180, *t*= 1.737, *p*<0.10).

5. Discussion and Conclusion

The actions or inactions of organizations are integral contributor to successful deployment of their services. Additionally, organizational actions affect individuals' willingness to use services or technology. Understanding how organizations respond to individual concerns about their technology especially under crisis condition is critical to the success of the technology. We focused on the success of protective technologies use following privacy violation crisis.

Prior studies on the factors that promote the use of technology generally suggest, among other factors, ease of use, usability, trust and personal disposition as good predictors of systems use [15, 31, 38]. However, when users experience violation of their privacy, trust may be waned, ease of use and usability may become secondary to users' consideration. Individuals' judgment on privacy violation crisis determines their subsequent behavioral reaction or decision-making [41]. We bring that important aspect of technology use decision-making into focus. We explore individuals' judgmental processes in responding to protective technologies offered as part of crisis management. An important question that organizations, such as Facebook, confront following the discovery of a breach is whether their users will use their platform or promoted protective technologies/services. Currently there is no empirical evidence that suggests users will be willing to use such services or find them useful. Furthermore, there is no understanding of whether the organization post data breach actions influence the use of protective technologies. We argued that, two key dimensions of organization justice theory – procedural justice and informational justice – would influence the likelihood of use of protective technologies. Our parsimonious preliminary empirical investigation rendered clear support for our core hypotheses that, increase in users' perception of procedural justice and information justice are good predictors of protective technologies use, even after controlling for user experience, age and general privacy concerns. This is particularly true in the context of Facebook's CHT.

It implies that user perceptions of fairness of the actions or evaluation of the processes involved in arriving at the decision in dealing with crisis affects their positive judgement of the organization. Users place premium on the actions taken to protect them from future violation or provide relief from the current breach. Such an outlook by users will increase their trust in the protective services offered by the violating entity. Hence, any concerns about protective technologies are lowered, allowing the user to use protective technologies. In addition, fair information practices such as timely and honest provision of detail information about a breach and actions to be taken empower users to take the necessary steps to secure their private information. This enhances users' perceptions of the organization's information justice and signals that the organization values and takes them seriously. Taken together, users' perception of whether they are fairly treated by the organization influence their perception of the usefulness of protective technologies.

However, the stronger effect of procedural justice in our research suggests that, actions indeed speaks louder than words. Procedural justice strengthens information justice as users observe alignment between the information provided and actions taken to ensure users are protected from future violation. This is consistent with prior research on behavioral integrity that suggests that users view words without actions as cheap talk on the part of the violating entity [18].

Our findings have both theoretical and practical implications. Theoretically, we found that in the context of using protective technologies, justice perceptions complement previously established important predictors of systems use. The finding is consistent with Culnan and Armstrong's [14] argument that procedural justice is a promising theoretical basis for future research on information privacy. This is because fairness appears to be a key factor in addressing users' concerns after privacy violation.

For managers, our findings suggest that when information and procedures enactment are separate, it is procedural justice that plays a dominant role in influencing users' desire to use or adopt services to protect themselves. This is because while informational justice ensures that users have trust regarding the data available, it is the fairness of the procedures that elicit trust in the platform operator. Fairness in the decision-making process and actions to protect users' privacy signals the violated users that, the platform operator is serious about the need to resolve the privacy crisis [9].

Our research is not without limitation. First, we did not examine other dimensions of organizational justice theory – distributive justice and interactional justice. This limitation is as result of our study context. Future research may explore these other dimensions along with the dimensions investigated in this study in other contexts where all dimensions exist, to test the efficacy of organizational justice theory in explaining protective technology use. For methodology, we employed Harman's single factor approach to examine the presence of common method variance. Future research may employ other techniques such as the marker variable approach to strengthen the validity of the findings. Despite these limitations, our study provides an initial theoretical investigation into post data breach use of technologies that have implications for research and managers.

12. References

[1] Armerding, T., "The 17 Biggest Data Breaches of the 21st Century", 2018. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

[2] Ayaburi, E.W., and D.N. Treku, "Effect of penitence on social media trust and privacy concerns: The case of Facebook", International Journal of Information Management 50, 2020, pp. 171–181.

[3] Bansal, G., and F.M. Zahedi, "Trust violation and repair: The information privacy perspective", Decision Support Systems 71, 2015, pp. 62–77.

[4] Bhattacherjee, A., "Understanding Information Systems Continuance: An Expectation-Confirmation Model", MIS Quarterly 25(3), 2001, pp. 351.

[5] Chen, H., C.E. Beaudoin, and T. Hong, "Teen online information disclosure: Empirical testing of a protection motivation and social capital model", Journal of the Association for Information Science and Technology 67(12), 2016, pp. 2871–2881.

[6] Chenoweth, T., R. Minch, and T. Gattiker, "Application of Protection Motivation Theory to Adoption of Protective Technologies", nd Hawaii International Conference on System Sciences, 2009, pp. 10.

[7] Chin, W.W., A. Gopal, and W.D. Salisbury, "Advancing the theory of adaptive structuration: The development of a scale to measure faithfulness of appropriation", Information systems research 8(4), 1997, pp. 342–367.

[8] Chin, W.W., B.L. Marcolin, and P.R. Newsted, "A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study", Information systems research 14(2), 2003, pp. 189–217.

[9] Chiu, C.-M., H.-Y. Lin, S.-Y. Sun, and M.-H. Hsu, "Understanding customers' loyalty intentions towards online shopping: an integration of technology acceptance model and fairness theory", Behaviour & Information Technology 28(4), 2009, pp. 347–360.

[10] Cohen, J., P. Cohen, S.G. West, and L.S. Aiken, Applied multiple regression/correlation analysis for the behavioral sciences., Routledge, 2013.

[11] Colquitt, J.A., J.A. LePine, R.F. Piccolo, C.P. Zapata, and B.L. Rich, "Explaining the justice–performance relationship: Trust as exchange deepener or trust as uncertainty reducer?", Journal of Applied Psychology 97(1), 2012, pp. 1–15.

[12] Colquitt, J.A., and J.B. Rodell, "Justice, Trust, and Trustworthiness: A Longitudinal Analysis Integrating Three Theoretical Perspectives", Academy of Management Journal 54(6), 2011, pp. 1183–1206.

[13] Crossler, R.E., F.K. Andoh-Baidoo, and P. Menard, "Espoused cultural values as antecedents of individuals' threat and coping appraisal toward protective information technologies: Study of U.S. and Ghana", Information & Management 56(5), 2019, pp. 754–766.

[14] Culnan, M.J., and P.K. Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation", Organization Science 10(1), 1999, pp. 104–115.

[15] Davis, F.D., R.P. Bagozzi, and P.R. Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models", Management Science 35(8), 1989, pp. 982–1003.

[16] Dinev, T., J. Goo, Q. Hu, and K. Nam, "User behaviour towards protective information technologies: the role of national cultural differences", Information Systems Journal 19(4), 2009, pp. 391–412.

[17] Dinev, T., and Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies", Journal of the Association for Information Systems 8(7), 2007, pp. 386–408.

[18] Dirks, K.T., P.H. Kim, D.L. Ferrin, and C.D. Cooper, "Understanding the effects of substantive responses on trust following a transgression", Organizational Behavior and Human Decision Processes 114(2), 2011, pp. 87–103.

[19] Greenberg, J., "Organizational justice: Yesterday, today, and tomorrow", Journal of management 16(2), 1990, pp. 399–432.

[20] Hair, J.F., J.J. Risher, M. Sarstedt, and C.M. Ringle, "When to use and how to report the results of PLS-SEM", European Business Review 31(1), 2019, pp. 2–24.

[21] Junglas, I.A., N.A. Johnson, and C. Spitzmüller, "Personality traits and concern for privacy: an empirical study in the context of location-based services", European Journal of Information Systems 17(4), 2008, pp. 387–402.

[22] Lai, F., D. Li, and C.-T. Hsieh, "Fighting identity theft: The coping perspective", Decision Support Systems 52(2), 2012, pp. 353–363.

[23] Li, H., R. Sarathy, J. Zhang, and X. Luo, "Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance: Determinants of IUP compliance", Information Systems Journal 24(6), 2014, pp. 479–502.

[24] Lowry, P.B., J. D'Arcy, B. Hammer, and G.D. Moody, "'Cargo Cult' science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels", The Journal of Strategic Information Systems 25(3), 2016, pp. 232–240.

[25] Muncaster, P., "Over a Third of Global Firms Breached in 2017", 2018. https://www.infosecurity-magazine.com/news/over-a-third-of-global-firms/

[26] Näsi, M., P. Räsänen, T. Keipi, and A. Oksanen, "Trust and victimization: A cross-national comparison of Finland, the U.S., Germany and UK", Research on Finnish society 10, 2017, pp. 13.

[27] Ng, B.-Y., A. Kankanhalli, and Y. (Calvin) Xu, "Studying users' computer security behavior: A health belief perspective", Decision Support Systems 46(4), 2009, pp. 815–825.

[28] Perlroth, N., A. Tsang, and A. Satariano, "Marriott Hacking Exposes Data of Up to 500 Million Guests", The New York Times, 2018. https://www.bbc.com/news/technology-46401890

[29] Podsakoff, P.M., S.B. MacKenzie, J.-Y. Lee, and N.P. Podsakoff, "Common method biases in behavioral research: A critical review of the literature and recommended remedies.", Journal of Applied Psychology 88(5), 2003, pp. 879–903.

[30] Ringle, C.M., S. Wende, and J.-M. Becker, SmartPLS 3. Bönningstedt: SmartPLS, 2015.

[31] Rogers, E.M., Diffusion of innovations, Free Press, New York, 1995.

[32] Rogers, E.M., "A Prospective and Retrospective Look at the Diffusion Model", Journal of Health Communication 9(sup1), 2004, pp. 13–19.

[33] Simons, T., "Behavioral Integrity: The Perceived Alignment Between Managers' Words and Deeds as a Research Focus", Organization Science 13(1), 2002, pp. 18–35.

[34] Sindhav, B., J. Holland, A.R. Rodie, P.T. Adidam, and L.G. Pol, "The Impact of Perceived Fairness on Satisfaction: Are Airport Security Measures Fair? Does it Matter?", Journal of Marketing Theory and Practice 14(4), 2006, pp. 323–335.

[35] Stern, T., and N. Kumar, "Improving privacy settings control in online social networks with a wheel interface: Improving Privacy Settings Control in Online Social Networks with a Wheel Interface", Journal of the Association for Information Science and Technology 65(3), 2014, pp. 524–538.

[36] Symantec, "Internet Security Threat Report", 23, 2018. https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[37] Tomlinson, E.C., and R.C. Mayer, "The Role of Causal Attribution Dimensions in Trust Repair", The Academy of Management Review 34(1), 2009, pp. 85–104.

[38] Venkatesh, V., M.G. Morris, G.B. Davis, and F.D. Davis, "User Acceptance of Information Technology: Toward a Unified View", MIS Quarterly 27(3), 2003, pp. 425–478.

[39] Willison, R., M. Warkentin, and A.C. Johnston, "Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives: Examining the influence of disgruntlement on computer abuse intentions", Information Systems Journal 28(2), 2018, pp. 266–293.

[40] Wong, J.C., "The Cambridge Analytica scandal changed the world – but it didn't change Facebook", The Guardian, 2019.

[41] Wright, R.T., and K. Marett, "The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived", Journal of Management Information Systems 27(1), 2010, pp. 273–303.

Appendix: Survey Instrument and loadings

	Items	IJ	LK	PC	PJ
	Information Justice				
IJ1	Facebook has been candid in communicating its action after privacy violation announcement	0.86	0.28	-0.20	0.60
IJ2	Facebook explained its procedure thoroughly after privacy violation announcement	0.90	0.28	-0.17	0.59
IJ3	Facebook’s explanations after privacy violation announcement is reasonable	0.88	0.30	-0.14	0.54
IJ4	Facebook communicated details in a timely manner after privacy violation announcement	0.86	0.23	-0.26	0.55
IJ5	Facebook seemed to tailor communications to individuals’ specific needs	0.81	0.34	-0.18	0.51
	Procedural Justice				
PJ1	Facebook’s decisions, after privacy violation announcement, were influenced by its users	0.34	0.20	0.04	0.57
PJ2	Facebook’s actions about the privacy violation were consistent	0.62	0.28	-0.12	0.80
PJ3	Facebook's actions about the privacy violation were free of bias	0.56	0.31	-0.07	0.80
PJ4	Facebook’s actions about the privacy violation were based on accurate information	0.40	0.38	0.01	0.77
	Likelihood of Use				
LK1	I am comfortable using Facebook’s clear history tool to delete my information	0.39	0.82	-0.04	0.42
LK2	I am likely to use Facebook’s clear history tool to delete my information	0.24	0.88	0.20	0.26
LK3	I will like to use Facebook’s clear history tool to manage my information	0.24	0.92	0.18	0.37
	Control Variables				
	General Privacy Concerns				
PC1	I am sensitive about giving out information regarding my preferences on online sites	-0.20	0.04	0.59	-0.07
PC2	I am concerned about anonymous information collected about me	-0.17	0.01	0.70	-0.08
PC3	I am concerned about how my personal unidentifiable information (information that I have voluntarily given out but cannot be used to identify me, e.g., Zip Code, age-range, sex, etc.) will be used by online sites	-	-	-	-
PC4	I am concerned about how my personally identifiable information (information that I have voluntarily given out AND can be used to identify me as an individual, e.g., name, shipping address, credit card or bank account information, social security number, etc.) will be used by online sites	-0.191	0.133	0.973	-0.031
	Age *(please enter your age in years*				
	Experience How long have you been using Facebook? Do you believe you were affected by the Facebook/Cambridge Analytica privacy violation				